Registre Telemàtic per Administracions Públiques

Universitat de Lleida
Escola Politècnica Superior

Autors: Josep Maria Mirada Donisa
Jordi Cerezo Garcia

Tutor: Francesc Solsona Tehas

Resum

Les Administracions Públiques són el conjunt d'organitzacions de caràcter públic que realitzen funcions administratives i de gestió dels diversos òrgans de govern, tant estatals com regionals i locals. Entre les seves funcions, s'inclou la posada en contacte i interacció de la ciutadania amb les entitats públiques. Aquestes interaccions s'han de fer presencialment, obligant al ciutadà a personar-se a les corresponents oficines per realitzar qualsevol tràmit, o entregar la documentació requerida per dur-lo a terme. Això suposa un cost, no només econòmic, si no de temps i volum de feina, tant per al ciutadà com per a l'Administració Pública.

El projecte neix amb la finalitat de reduir aquests costos, creant una infraestructura que permeti realitzar els tràmits amb les Administracions Públiques per via telemàtica. D'aquesta forma se suprimeix la necessitat d'acudir presencialment a una oficina de l'Administració, suposant una gran avantatge per ambdues parts, especialment en quant al cost temporal.

Els diferents tràmits que necessita realitzar un ciutadà amb una Administració Pública requereixen de la seva signatura. En el cas que el tràmit es faci de forma presencial, el ciutadà pot signar en persona aquests documents. Però si es duen a terme per via telemàtica, es fa imprescindible dotar a l'aplicació d'un mecanisme per realitzar aquesta signatura, i que gaudeixi de la mateixa validesa que una signatura manuscrita. Sorgeix així la necessitat d'implementar un sistema de signatura digital per a atorgar validesa als tràmits per via telemàtica.

Aquests sistemes de signatures digitals s'implementen utilitzant les claus públiques i privades que contenen els certificats electrònics. Es fa necessari, doncs, algun tipus de certificat que tota persona tingui o pugui obtenir fàcilment. És per aquest motiu que es fa òptima la utilització del DNI electrònic, donat que és un document del qual tothom disposa de manera obligatòria i que conté els certificats que permeten realitzar aquests tipus de signatures digitals.

Índex de continguts

1 Introducció

Actualment, la ciutadania té a la seva disposició nombroses Administracions Públiques, representants de diversos òrgans de govern, que li permeten la realització de tota mena de gestions, ja siguin tràmits legals, consultes d'informació, diferents sol·licituds o permisos.....

El volum de dades i de feina que generen aquestes tramitacions a les Administracions és considerable. A més, basen la seva feina de forma habitual en l'ús de documents oficials impresos en paper. Això implica l'ús de segells legals i signatures vàlides per als registres d'entrada i sortida de documents, tràmits, o qualsevol altre tipus d'acció o informació.

Aquesta infraestructura i forma de treballar, en la que es depèn de documents oficials impresos en paper, genera un gran cost, tant a nivell econòmic com en quant a volum de feina. El document ha de ser entregat de forma presencial per la persona interessada, creant la necessitat de realitzar un desplaçament cap a la seu de la corresponent Administració, i aquest document ha de ser admès, i validat de forma física pels treballadors autoritzats. El document ha de ser signat pel ciutadà de forma manuscrita, i segellat pel treballador, per tal d'atorgar-li validesa legal.

Aquest projecte intenta donar resposta a la necessitat de crear una plataforma que suposi una millora notable respecte al funcionament tradicional de les Administracions Públiques. Amb aquest objectiu, es desenvolupa una aplicació web que implementa un Registre Telemàtic que permet que totes aquestes interaccions entre Administració Pública i ciutadania, puguin realitzar-se de forma remota, evitant costos econòmics i temporals. Davant de la necessitat de donar validesa als tràmits que permetrà emmagatzemar aquest registre digital, s'utilitzarà l'anomenada signatura digital. Aquesta requereix d'uns certificats electrònics, que podem trobar en diferents mitjans. La obligatorietat de tot ciutadà de disposar del DNI electrònic, facilita la decisió d'utilitzar-lo per a la realització de les signatures digitals, ja que es fa imprescindible emprar un document del qual disposi el màxim de ciutadans possible.

L'aplicació s'ha centrat en la realització de tràmits via telemàtica entre l'Administració Pública i els ciutadans. El fet d'implementar aquesta aplicació web en qualsevol Administració Pública implica un conjunt de millores que podem dividir en dues parts:

- Millores de caràcter intern. Si s'observa des del costat de l'administració pública, realitzar els tràmits online permet l'eliminació de documents en paper que suposa una disminució substancial del volum de feina, reduint el número de treballadors, el temps de gestió d'aquests tràmits i els costos en material (segells, folis, arxius, etc...)
- Millores de caràcter extern. Pels ciutadans, el fet que es puguin realitzar tràmits online suprimeix la necessitat de personar-se davant les administracions. A més, provoca una millora en la percepció d'immediatesa, ja que els tràmits poden ser realitzats i consultats en qualsevol moment del dia. Així, es pot gaudir d'informació gairebé instantània de l'estat en que es troben aquests tràmits.

1.1 Objectius

Objectius

- Crear una aplicació web que permeti als ciutadans interaccionar amb l'administració pública via telemàtica.

- Facilitar les tasques de gestió dels tràmits de l'administració reduint els costos i volum de feina.
- Aplicar la signatura digital en compliment de les polítiques de seguretat estàndard per a les comunicacions telemàtiques emprant el DNIe (document nacional d'identitat amb xip electrònic)
- Realitzar les signatures digitals amb el DNIe assegurant que es compleixin les seves característiques essencials; autenticació, integritat i no repudi.
- Dotar l'aplicació web d'un gestor documental on els usuaris puguin consultar tots els documents que han anat tramitant.

2 Bases de criptografia

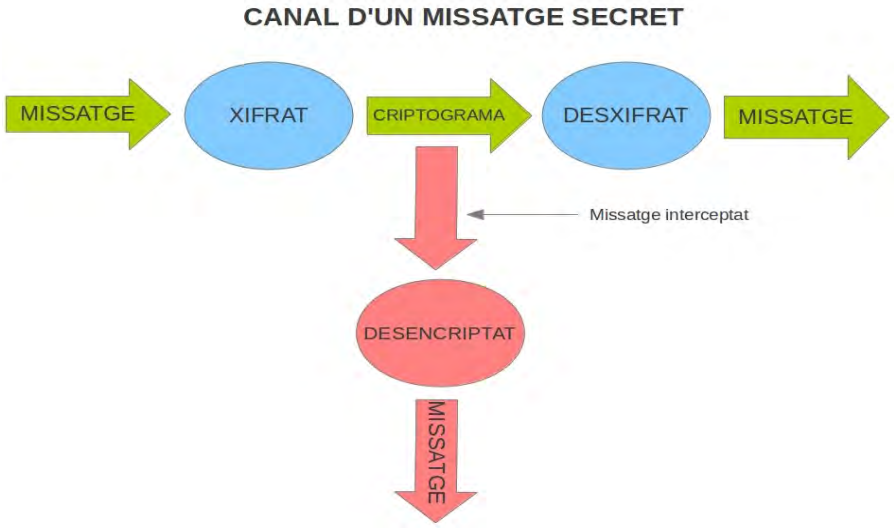
2.1 Introducció a la criptografia

Al llarg de la seva evolució, l'ésser humà ha desenvolupat la capacitat de comunicar-se amb els demés, permetent-li convertir-se en un ésser social capaç de transmetre informació als altres. Però gairebé des del mateix moment en que sorgeix la comunicació, sorgeix la necessitat d'ocultar aquesta informació als altres, i que sigui entesa únicament per determinats interlocutors.

La primera solució ideada fou la de la ocultació del propi missatge. Aquesta tècnica rep el nom d'esteganografia. Trobem exemples en la història, com la descripció del gran historiador grec Heròdot, que al segle V abans de Crist deixà escrita una tècnica que s'emprava a l'antiga Grècia, mitjançant la qual el missatge era escrit a una tauleta de fusta, i posteriorment recoberta amb cera. El mateix Heròdot narra una altra tècnica, atribuïda a Histaideus, que consistia en rapar el cap a un missatger, escriure el missatge al cuir cabellut, i esperar a que el cabell torni a créixer. A partir de llavors, el missatger podia viatjar a l'entrega del missatge, sense ser destorbat per enemics. Un cop arribava a la presència del destinatari del missatge, simplement rapant-se de nou el cap, es podia llegir la informació. Altres tècniques més depurades i modernes, foren emprades durant la Segona Guerra Mundial. La mida d'un text era reduïda fins al punt que era il·legible per a l'ull humà, i podia passar inclús per un signe de puntuació en un text més gran. Un punt d'una consonant “j” podia en realitat ser un microfilm amb un missatge de gran importància.

Però per molt bé que siguin ocultats els missatges, sempre hi ha el risc que siguin descoberts, i els seus secrets divulgats. Per aquest motiu, va sorgir una tècnica molt més sofisticada que no intentava ocultar el text, si no més aviat el contingut del mateix: **la criptografia**.

La paraula criptografia prové dels termes grecs “**criptos**”, ocult, i “**grafos**”, escriptura. Així, com el seu propi nom indica, la criptografia és la tècnica de la escriptura secreta, sistemes de xifrat, que permeten, mitjançant algunes transformacions, ocultar el missatge, i que pugui ser llegit posteriorment, només aplicant el sistema de desxifrat. D'aquesta forma, es permet una comunicació segura entre dos interlocutors, de tal manera que només ells dos són els coneixedors de la informació que conté el missatge xifrat, quedant oculta aquesta a la resta de persones (Il·lustració 1).



Il·lustració 1: Diagrama de comunicació mitjançant un canal segur

Com s'ha comentat, la criptografia es centra en tècniques que permeten la ocultació de la informació. Però juntament amb aquest intent d'ocultació, van sorgir les anomenades tècniques de criptoanàlisi, mecanismes emprats per a descodificar la informació i trencar els mecanismes de xifrat.

Malauradament,i com en molts altres camps de la ciència i el coneixement, són les guerres les que han provocat els majors avenços en aquesta disciplina, per poder servir els propòsits dels diferents bàndols enfrontats. La major part dels sistemes criptogràfics, s'han desenvolupat en períodes de guerra.

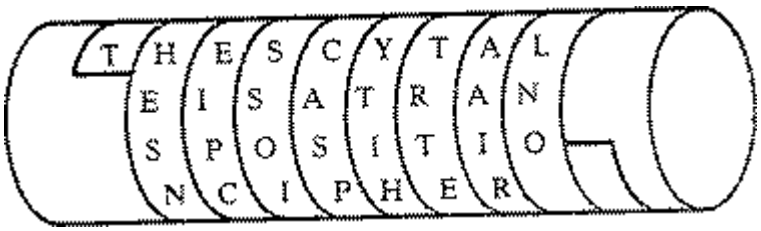
Actualment, i amb els grans avenços que s'han produït en el camp de la informàtica i de les telecomunicacions, les tècniques criptogràfiques han passat a ser molt necessàries, fent-se servir en tota mena d'activitats comunes, com les transaccions per Internet, o l'autenticació personal mitjançant la signatura digital.

2.2 Criptografia simètrica o de clau secreta

2.2.1 Criptografia clàssica

Els primers exemples de criptografia a la història daten del segle V abans de Crist i van ser utilitzats pels espartans. Era un mètode molt simple que consistia en enrotllar una cinta de cuir o un papir a una vara, anomenada **escítala (**Il·lustració 2**)**, s'escrivia el missatge de forma longitudinal, i un cop fet, es desenrotllava el papir, donant com a resultat una cinta amb lletres arbitràries i sense sentit. La clau d'encriptació en aquest cas era tan simple com el diàmetre de l'**escítala**, que equivalia al nombre de lletres que cabien a cada volta del papir a la vara (Il·lustració 3). Era un mètode rudimentari, però donada la manca de cultura general, i el poc coneixement d'idiomes, resultava un mètode prou segur a la època.

Il·lustració 2: L'escítala



Il·lustració 3: Exemple de xifrat amb l'escítala

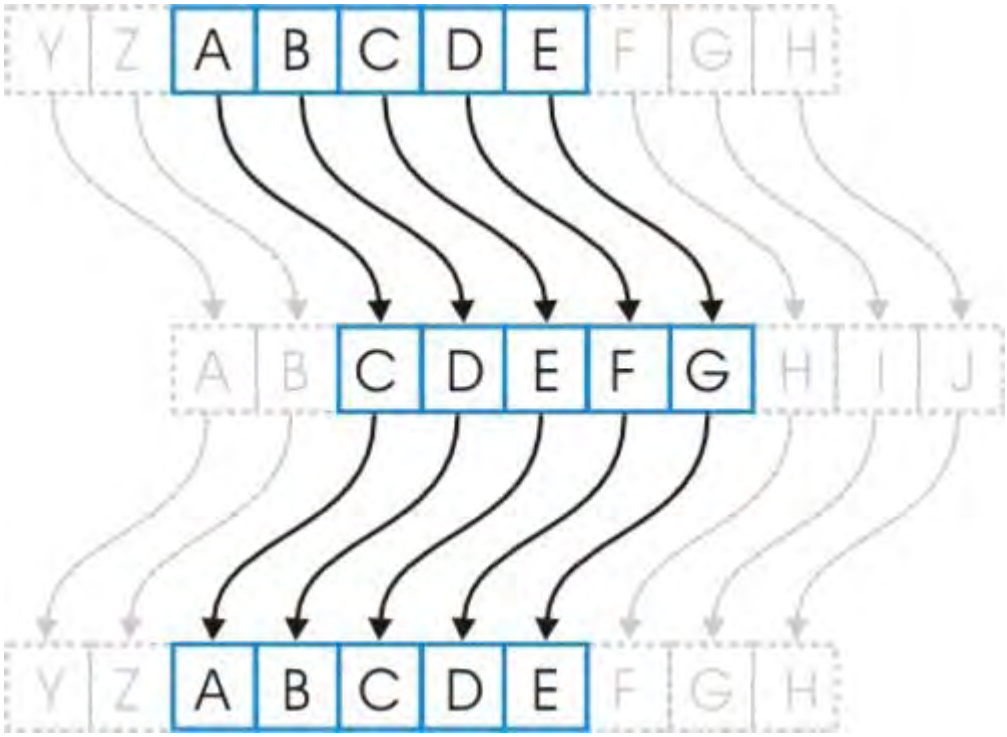
El següent sistema d'encriptació data del segle I A.C. i va ser el primer sistema a la història que emprava la tècnica de substitució de caràcters. Es tracta del **xifrador de Polybius (**Il·lustració 4**)**. En una petita taula es col·locaven els símbols de l'alfabet, i es substituïa cadascun d'ells per la fila i columna que l'identificava a la taula. D'aquesta manera, la única manera de poder desxifrar el missatge era saber en quina fila i columna de la taula es trobava cada caràcter, i realitzar la substitució.

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Il·lustració 4: Taula de Polybius

Per tal de xifrar el missatge, se substituïa cadascuna de les lletres pel parell fila/columna corresponent. D'aquesta manera s'aconseguia reduir el nombre de caràcters finals, permetent la manipulació dels dos de forma independent.

Posteriorment, durant el mateix segle I A.C. **Juli Cèsar** (Il·lustració 5) va inventar un codi per a amagar els seus missatges. La tècnica consistia en la substitució de cadascun dels caràcters del missatge, pel caràcter resultant de desplaçar tres posicions a la dreta a l'alfabet (la A passava a ser la D, la B passava a ser la E, i així successivament). La clau d'encriptació era precisament aquest **desplaçament**. D'aquesta manera, es podria depurar la tècnica, canviant el nombre de posicions a desplaçar al llarg de l'alfabet, o inclús substituint cada caràcter per un de donat, i que no fos resultat d'un desplaçament, si no d'una assignació arbitrària.



Il·lustració 5: Criptosistema de Juli Cèsar

Un cop vistes aquestes pinzellades de criptografia clàssica, passarem a veure altres sistemes emprats amb posterioritat.

2.2.2 Criptografia simètrica moderna

2.2.2.1 Criptosistemes anteriors a la Segona Guerra Mundial

El període de temps que va del segle I D.C. i fins al segle XV D.C. és considerat com la "Era fosca de la criptografia". Durant aquests segles, no es van produir gairebé avenços en termes criptogràfics, i durant alguns períodes fou considerada com màgia fosca, i per tant, aquesta disciplina tenia una consideració molt dolenta.

Durant el segle XV D.C. es va produir el més remarcable avenç criptogràfic fins a la II Guerra Mundial. Concretament l'any 1465, **Leon Battista Alberti** ideà el primer sistema criptogràfic **polialfabètic** del que es té coneixement. El funcionament d'aquest sistema estava basat en la utilització d'uns **discos concèntrics** en els qual es representava l'alfabet (Il·lustració 6). Emissor i receptor havien de posar-se d'acord en la posició relativa dels discos, determinant així la correspondència entre els caràcters. A més, i cada n paraules, també prefixades pels interlocutors, es canviava l'alfabet que s'emprava. Cadascun dels caràcters del missatge en clar es substituïa per la seva correspondència al disc interior, xifrant d'aquesta manera el missatge.

Il·lustració 6: Disc d'Alberti

Molts dels sistemes de xifratge posteriors, van tenir a veure amb la competència política i la Revolució religiosa, però, en general, denotaven poc enteniment, o directament desconeixement del sistema polialfabètic dissenyat per Alberti. Però si podem destacar-ne uns quants que són molt posteriors a la època d'Alberti, però anteriors a la II Guerra Mundial.

Al 1585 el diplomàtic francès **Blaise de Vigenère** va publicar el llibre "**Tractié de Chiffre**". Aquí presentava el primer sistema polialfabètic amb clau privada o secreta, idea que perdurarà en el temps, i s'aplicarà a futurs algoritmes moderns. Aquest sistema feia anar com a element principal

una taula anomenada **Taula de Vigenère**. (Il·lustració 7)

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
W	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Il·lustració 7: Taula de Vigenère

Per a l'encriptació de les dades, s'havia de dividir el missatge en blocs de la mateixa mida (mateix nombre de caràcters) que la clau emprada. Aplicant la clau a cadascun dels blocs en que s'havia dividit el missatge, s'havia de triar la lletra que ens donava la taula, de tal forma que se seleccionava la columna segons el caràcter corresponent del bloc del missatge original, i la fila, segons el caràcter marcat per la clau emprada.

Per exemple, si el missatge a encriptar fos: **Xifrat de Vigenere**. I la clau fos: **Prova**.

x	i	f	r	a	t	d	e	v	i	g	e	n	e	r	e
p	r	o	v	a	p	r	o	v	a	p	r	o	v	a	p
m	z	t	m	a	i	u	s	q	i	v	v	b	z	r	t

El missatge xifrat serà, doncs: **mztmaiusqivvbzrt**.

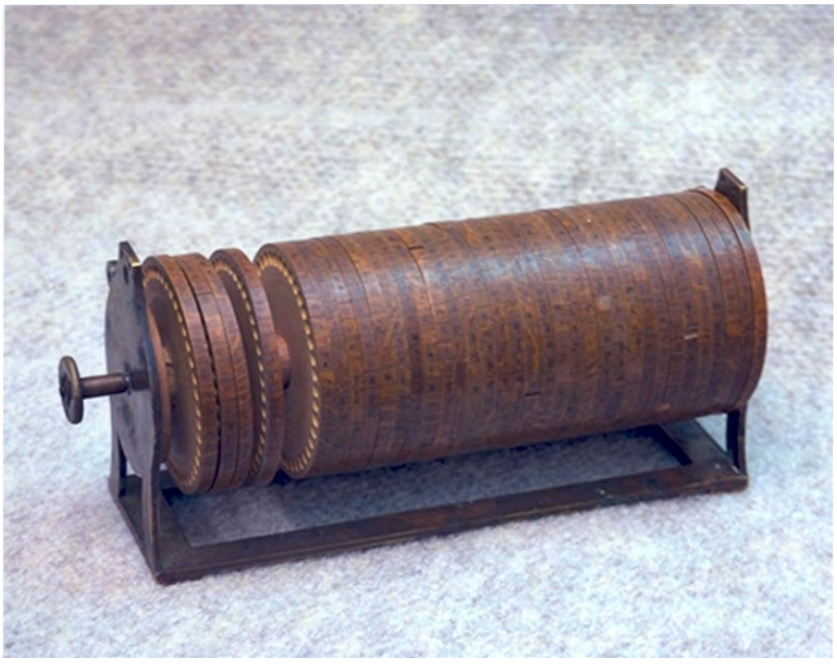
Aquest xifratge polialfabètic va ser considerat invulnerable fins que, al segle XIX es van aconseguir desxifrar alguns missatges mitjançant l'anàlisi de repeticions de blocs de lletres, ja que la distància entre un bloc i la seva repetició sol ser múltiple de la paraula pressa com a clau.

El segon xifratge de Vigenère és similar al primer. La codificació del text es realitza de la mateixa forma, amb la diferència de la clau a utilitzar. Si al primer tipus de xifrat, la clau era la repetició de la paraula pressa com a clau de codificació, en aquest segon tipus de xifrat, inicialment la clau serà també una paraula arbitrària, però la **segona vegada**, en comptes de repetir aquesta paraula, s'agafarà la **part del missatge en clar** que s'ha utilitzat en la primera volta de la codificació.

Per exemple, si el missatge a xifrar fos: "**Aquest és el missatge en clar**", i la clau fos "**Prova**", xifraríem mitjançant la taula de Vigenère emprant "aques" (**aques**t es el missatge en clar) i "prova". En la següent volta, xifraríem la part "tesel" (aques**t es el** missatge en clar), i empraríem com a clau "aques" (**aques**t es el missatge en clar). En la tercera volta xifrariem la part del missatge "missa" (aquest es el **missa**tge en clar) emprant com a clau "tesel" (aques**t es el** missatge en clar), i així successivament.

Al segle XVIII **Francis de Beaufort**,crea un criptosistema que funciona anàlogament al criptosistema de Vigenère. Es tracta d'una **substitució de caràcters periòdica amb alfabets desplaçats**. La diferència és que, en aquest cas, s'invertia l'ordre de les lletres de l'alfabet, i després es desplaçaven a la dreta.

La **roda de Jefferson(**Il·lustració 8**)**, va ser inventada al 1790 per **Thomas Jefferson**, president i redactor de la declaració d'Independència dels Estats Units. Consistia en 26 rodes de fusta, cadascuna gravada amb les lletres de l'alfabet de forma desordenada i col·locades sobre un eix formant un cilindre. Cada roda tenia un ordre de caràcters diferents de la resta, i per xifrar un missatge, es col·locava el text en clar en una de les files, i qualsevol de les altres es podia utilitzar com a missatge xifrat. El receptor havia de posar el missatge xifrat rebut a una de les línies de les rodes, i buscar el missatge en clar a les altres. Com mai no va fer anar aquesta màquina, fou gairebé oblidada. Fins al 1890 quan **Étienne Bazeries**, prenent com a base el disc de Jefferson va crear un sistema molt similar. Constava de 20 discs coaxials amb 25 lletres cadascun, que el cilindre fou creat. Al tenir un disc addicional amb números, el missatge en clar es podia conformar amb lletres de diverses generatrius, establint el número de la generatriu amb que es xifrava cada caràcter del missatge en clar.



Il·lustració 8: Roda de Jefferson

El **disc de Wheatstone** (Il·lustració 9) fou creat al 1867 per **Sir Charles Wheatstone**. Es tractava d'una versió mecànica del sistema d'Alberti, però amb unes manetes que apuntaven als alfabets escrits als discs, de tal forma que donava la correspondència entre els dos alfabets concèntrics.

Il·lustració 9: Disc de Wheatstone

Un altre mètode de xifrat inventat per Sir Charles Wheatstone, fou l'**algoritme de Playfair**. S'anomena així, perquè fou el seu amic **Lyon Playfair**, primer baró Playfair de St. Andrews i amb qui es reunia sovint per intercanviar les seves idees sobre criptografia, el que el va popularitzar.

Aquest mètode, que no és polialfabètic, si no **poligràmic**, va ser utilitzat al Regne Unit durant la Primera Guerra Mundial. Consistia en la substitució de cada parell de lletres del missatge en clar per un altre parell de lletres. Emissor i receptor havien d'acordar primer una paraula clau. Seguidament, i abans de codificar, les lletres de l'alfabet s'havien d'escriure en un quadre de 5x5, i combinant les lletres **I** i **J** en un únic requadre (es podia afegir la paraula clau a l'inici de la matriu, en lloc de les primeres lletres).

Per tal de xifrar s'utilitzaven les següents regles (anomenarem un parell de lletres en clar **m1** i **m2**, i al parell resultant de la codificació, **c1** i **c2**):

- Si **m1** i **m2** són a la mateixa fila de la matriu, **c1** i **c2** seran les lletres que es troben a la dreta de **m1** i **m2**.
- Si **m1** i **m2** estan a la mateixa columna, **c1** i **c2** seran les lletres de sota de **m1** i **m2**.
- Si **m1** i **m2** estan en diferents files i columnes, **c1** i **c2** seran les lletres que estan a la mateixa distància de l'eix de simetria que **m1** i **m2**, a la seva mateix fila.
- Si **m1** es igual a **m2**, s'insereix una lletra considerada com nul·la (per exemple una X) per eliminar la duplicitat.
- Si el text en clar té un nombre parell de caràcters, s'afegeix un considerat nul (per exemple la X) al final del missatge.

Com a exemple, xifrem el text "**Codi de Playfair**" amb aquest mètode:

- Co: **m1** i **m2** pertanyen a files i columnes diferents, **c1** i **c2** seran C i M.
- di: **m1** i **m2** pertanyen ala mateixa columna, **c1** i **c2** seran I i O.
- de: **m1** i **m2** pertanyen a la mateixa fila, **c1** i **c2** seran E i A.
- pl: **m1** i **m2** pertanyen a la mateixa fila, **c1** i **c2** seran L i M
- ay: **m1** i **m2** pertanyen a files i columnes diferents, **c1** i **c2** seran E i W.
- Fa: **m1** i **m2** pertanyen ala mateixa columna, **c1** i **c2** seran L i F.
- Ir: **m1** i **m2** pertanyen a files i columnes diferents, **c1** i **c2** seran G i T.

El missatge xifrat seria: **CMIO EA LMEWLFGT**.

El receptor podia desxifrar el codi simplement invertint el procés. Si es troben a la mateixa fila, s'agafarien les lletres de l'esquerra, si estan a la mateixa columna, s'agafarien les de dalt, i si no estan ni a la mateixa fila ni columna, la seva corresponent segons l'eix de simetria.

Playfair va insistir en les bondats d'aquest mètode, aconseguint que l'oficina de guerra britànica l'adoptés per al xifrat de texts, i va funcionar durant un temps, però finalment es va demostrar poc robusta, perquè es podia atacar mitjançant un **anàlisi dels dígrafs més comuns** de la llegua que s'estava emprant per la comunicació, en aquest cas l'anglès.

El **xifrat de Hill** sorgeix al 1929 amb la publicació d'un article a Nova York per part de **Lester S. Hill**. Aquest proposà l'ús de les regles d'**àlgebra de matrius** a les tècniques criptogràfiques.

El mètode es basava en l'àlgebra lineal, i va ser important a la història de la criptografia, perquè va ser el primer sistema pràctic per treballar amb més de tres símbols simultàniament. Es pot considerar un sistema **polialfabètic**, donat que un mateix caràcter en un missatge a enviar, podia ser encriptat en dos caràcters diferents al missatge encriptat.

Posarem un exemple. Treballant amb l'alfabet habitual de 26 caràcters fem la següent assignació:

Alfabet inicial	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Valor numèric	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Es tria un nombre sencer '**d**', que determina blocs de **d** elements que són tractats com un vector de **d** dimensions.

Es tria de forma aleatòria una matriu **A** de de **d** x **d** elements, els quals seran la clau a emprar. Els elements de la matriu **d** x **d** seran sencers entre 0 i 25, i a més, la matriu **A** ha de ser invertible en $\mathbb{Z}_{26}^{n}$.

Per a l'encriptació, el text es dividit en blocs de **d** elements, els quals es multipliquen per la matriu **d** x **d**. Totes les operacions aritmètiques es realitzen en mòdul 26, és a dir, 26=0, 27=1, 28=2....

Per encriptar un missatge, hem de dividir-lo en blocs $\mathbf{P_i}$ de '**d**' caràcters, i aplicar:

$M \times P_i = C$, on **C** és el codi xifrat per al missatge $\mathbf{P_i}$.

Farem un exemple, on **d**=3.

Prenem aquesta matriu $A = \begin{bmatrix} 5 & 17 & 20 \\ 9 & 23 & 3 \\ 2 & 11 & 13 \end{bmatrix}$ com a matriu de claus. Aquesta matriu ha de ser invertible en modul 26. hi ha una manera relativament senzilla d'esbrinar-ho, a través del determinant de la matriu. Si el determinant de la matriu és 0, o té factors comuns amb el mòdul (en el cas del 26 els factors són 2 i 13), llavors la matriu no es pot utilitzar. Al ser 2 un dels factors de 26, hi haurà multitud de matrius que no puguin utilitzar-se (no es poden emprar ni les de determinant 0, un múltiple de 2 o un múltiple de 13).

Per constatar que és invertible, calculem el **determinant de A**:

$$A = \begin{bmatrix} 5 & 17 & 20 \\ 9 & 23 & 3 \\ 2 & 11 & 13 \end{bmatrix}$$

$5\,(23 \cdot 13 - 3 \cdot 11) - 17\,(9 \cdot 13 - 3 \cdot 2) + 20\,(9 \cdot 11 - 23 \cdot 2) = 1215 - 1734 + 1060 = 503$

$503 = 9 \bmod 26$

La matriu **A** és, doncs, invertible en mòdul 26, ja que 26 i 9 son coprimers. Per trobar la seva matriu inversa mòdul 26, emprem la fórmula $A^{-1} = C^T (det(A))^{-1}$ on C^T és la matriu de cofactors de **A** transposada. S'ha de tenir en compte que $(det(A))^{-1}$ s'ha de fer en mòdul 26, per tant, a l'exemple, la inversa de 9 (mod 26) és 3 (mod 26), ja que 9 (mod 26) · 3 (mod 26) = 1 (mod 26).

D'aquesta manera, sabem que 3 és la inversa multiplicativa de 9 en mòdul 26. Per calcular **C**, hem de calcular els cofactors de **A**:

$$C_{11} = +\begin{vmatrix} 23 & 3 \\ 11 & 13 \end{vmatrix} \quad C_{12} = -\begin{vmatrix} 9 & 3 \\ 2 & 13 \end{vmatrix} \quad C_{13} = +\begin{vmatrix} 9 & 23 \\ 2 & 11 \end{vmatrix}$$

$$C_{21} = -\begin{vmatrix} 17 & 20 \\ 11 & 13 \end{vmatrix} \quad C_{22} = +\begin{vmatrix} 5 & 20 \\ 2 & 13 \end{vmatrix} \quad C_{11} = +\begin{vmatrix} 23 & 3 \\ 11 & 13 \end{vmatrix}$$

$$C_{11} = +\begin{vmatrix} 23 & 3 \\ 11 & 13 \end{vmatrix} \quad C_{23} = -\begin{vmatrix} 5 & 20 \\ 9 & 3 \end{vmatrix} \quad C_{33} = +\begin{vmatrix} 5 & 17 \\ 9 & 23 \end{vmatrix}$$

$$A = \begin{bmatrix} 5 & 17 & 20 \\ 9 & 23 & 3 \\ 2 & 11 & 13 \end{bmatrix} \quad C^T = \begin{bmatrix} 266 & -1 & -409 \\ -111 & 25 & 165 \\ 53 & -21 & -38 \end{bmatrix}$$

Ara apliquem la fórmula inversa:

$$A^{-1}=C^{T}\left(det\left(A\right)\right)^{-1}=\begin{bmatrix}266 & -1 & -409\\ -111 & 25 & 165\\ 53 & -21 & -38\end{bmatrix}\cdot 3$$

$$A^{-1}=\begin{bmatrix}798 & -3 & -1227\\ -333 & 75 & 495\\ 159 & -63 & -114\end{bmatrix}\qquad A^{-1}=\begin{bmatrix}18 & 23 & 21\\ 5 & 23 & 1\\ 3 & 15 & 16\end{bmatrix}\left(mod\,26\right)$$

Aquesta serà la matriu que emprarem a posteriori per desencriptar.

Per encriptar el missatge "**llibre**", primerament separem el missatge en blocs de **d**=3 caràcters. Per tant, "**LLIBRE**" es converteix en "**LLI**" i "**BRE**".

$$P_1=LLI=\begin{bmatrix}12\\12\\9\end{bmatrix}\qquad\qquad P_2=BRE=\begin{bmatrix}2\\18\\5\end{bmatrix}$$

$$A\cdot P_1=\begin{bmatrix}5 & 17 & 20\\ 9 & 23 & 3\\ 2 & 11 & 13\end{bmatrix}\begin{bmatrix}12\\12\\9\end{bmatrix}=\begin{bmatrix}444\\411\\273\end{bmatrix}=\begin{bmatrix}2\\21\\13\end{bmatrix}\left(mod\,26\right)$$

Per tant, el primer bloc "**LLI**" serà codificat com "**BUM**".

$$A\cdot P_2=\begin{bmatrix}5 & 17 & 20\\ 9 & 23 & 3\\ 2 & 11 & 13\end{bmatrix}\begin{bmatrix}2\\18\\5\end{bmatrix}=\begin{bmatrix}416\\447\\267\end{bmatrix}=\begin{bmatrix}0\\5\\7\end{bmatrix}\left(mod\,26\right)$$

Per tant, la codificació del segon bloc "**BRE**" serà "**ZEG**".

Constatem doncs, que el missatge en clar "**LLIBRE**" ens dóna com a missatge codificat "**BUMZEG**".

Per desencriptar, el mètode és exactament el mateix, però emprant la matriu inversa que hem calculat anteriorment.

Altres màquines més modernes, i basades en rotors, foren dissenyades a partir del 1900. **Arthur Scherbius** i **Richard Ritter** inventaren, al 1918, la primera **Enigma** (Il·lustració 12, en parlarem en profunditat més endavant), que fou utilitzada durant la II Guerra Mundial. El sistema de xifratge va ser trencat per **Alan Turing** l'any 1940, utilitzant la **Bomba de Turing**, basant-se en el treball de **Marian Rejewski**. Les màquines de **Hagelin** (Il·lustració 11), van ser desenvolupades entre 1920 i 1930 pel criptòleg suec **Boris Hagelin**, basant-se en el sistema de xifrat de Beaufort. La màquina **M-325 (**Il·lustració 10), desenvolupada per **Frederick Friedman**, als anys 40 del segle XX era similar a la màquina **Enigma**, ja que també es basava en rotors.

Il·lustració 10: M-325

Il·lustració 11: Hagelin

Il·lustració 12: Enigma

2.2.2.2 Enigma i Alan Turing

Com s'ha comentat anteriorment, els enginyers alemanys **Arthur Scherbius**, un expert en electromecànica, i **Richard Ritter**, van patentar al 1918 una màquina de xifratge basada en el **xifrat de Vigenère**, (algoritme de substitució d'unes lletres per unes altres, que comentarem amb posterioritat), anomenada **Enigma** (Il·lustració 13). La manca de recursos econòmics per dur a terme la seva fabricació, va fer que **Arthur Scherbius** s'associes amb **Willie Korn**, propietari de la companyia **Enigma Chiffiermaschinen AG** de Berlín. Entre els dos van millorar el disseny, i van presentar la màquina a la Exhibició Postal de Berlín a l'any 1923, on es presentaven avenços pel xifratge de secrets empresarials i comercials.

Il·lustració 13: Enigma

Aquesta màquina fou de vital importància durant la **Segona Guerra Mundial**, un dels períodes històrics on la criptografia fou més important. Les comunicacions secretes es van convertir en un

més dels fronts de batalla, i es van dedicar grans esforços al desxifrat dels codis enemics. L' exercit alemany va començar a utilitzar la **Enigma** per la encriptació de les seves comunicacions, donant un **clar avantatge** a les tropes nazis, especialment als seus submarins, interceptant materials transportats des dels Estats Units a través de l'Atlàntic Nord. Per aquest motiu, les tropes aliades van considerar **prioritari el desxifrat de la Enigma**.

La màquina **Enigma** era un aparell **electromecànic**, és a dir, tenia una part elèctrica, i una part mecànica. La seva aparença era molt similar a la d'una màquina d'escriure convencional, i de fet, la forma en que s'havia d'utilitzar era gairebé la mateixa. Tot i que interiorment, les tecles accionaven la part elèctrica, que produïa el moviment dels seus rotors. L'usuari escrivia cadascun dels caràcters del missatge amb el teclat, i anotava la lletra retornada pel dispositiu a través d'un altre teclat que s'il·luminava. El codi venia donat per la **posició inicial dels rotors**, els quals tenien 26 cables que s'unien a les tecles. La gran particularitat era que el primer rotor donava una vint-i-sisena part de volta després de cada pulsació, generant una nova configuració de les connexions a cada caràcter. D'aquesta manera, el xifrat era polialfabètic. Però a més, quan el primer rotor donava una volta completa, el segon també feia una vint-i-sisena part de volta, i el tercer rotor la feia quan el segon completava la seva volta. Si a tot això li afegim la possibilitat d'intercanviar l'ordre dels rotors, la quantitat d'alfabets disponibles era de 105.456, cosa que, a la època, dotava a la Enigma d'una gran robustesa.

A més dels cilindres, la màquina disposava de 6 cables, que permetien afegir modificacions ja que es podien introduir a 26 entrades diferents, que eren representades per les lletres de l'alfabet de la Enigma, produint 100.391.791.500 possibilitats de connectar els cables. Creuant aquesta dada amb els 105.456 alfabets, es generaven 3.283.883.513.796.974.198.700.882.069.882.752.878.379.955.261.095.623.685.444.055.315.226.006.433.616.627.409.666.933.182.371.154.802.769.920.000.000.000 possibilitats de connexió diferents.

Fou al 1933 quan Alemanya va decidir nacionalitzar la empresa Enigma Chiffiermaschinen AG i va dotar a l'exèrcit alemany d'aquestes màquines de xifrat, a la que van afegir, al 1942, i en ple conflicte, un quart rotor per augmentar encara més la seguretat. D'aquesta manera, durant els primers anys de la Segona Guerra Mundial l'exercit alemany va gaudir d'un gran avantatge sobre els aliats. El **codi** a emprar per a les comunicacions **canviava diàriament**, i el codi de cada dia s'enviava a l'inici de les comunicacions, encriptat amb el codi del dia anterior. Això feia que els aliats disposessin únicament de 24h per a desxifrar les comunicacions. Quan es podia desxifrar el missatge enviat un determinat dia, probablement ja es tractava d'informació inútil, o desfasada. A més, cadascun dels diferents exercits tenien el seu propi codi diari.


Il·lustració 14: Marian Rejewski

La màquina **Enigma** s'aconseguí desxifrar gràcies a una sèrie de factors. El primer i més obvi, era que, en els seus inicis, era un model comercial, que va ser distribuït lliurement, així que el seu funcionament ja era conegut. A més, la codificació obligava a introduir 3 lletres, dues vegades, a l'inici del missatge, com una bandera. La Luftwaffe no modificava aquesta seqüència, i per tant era un patró que no s'alterava. **Marian Rejewski** (Il·lustració 14), un jove matemàtic polac, va aprofitar aquesta debilitat

per a trencar la **Enigma** utilitzant **tècniques fonamentals de matemàtiques i estadística**. Va crear unes màquines electromecàniques, que anaven comprovant diferents combinacions de codis de forma automatitzada. Aquestes van adquirir el sobrenom de “bombes”, degut al constant soroll de TIC TAC que feien els relés per canviar les seves posicions per fer les comprovacions de codis.

Al 1940, i per tal de trencar el codi de la **Enigma**, el govern anglès, van reunir a una mansió victoriana a Bletchley, comtat de Buckingham-shire, a nou dels més brillants teòrics matemàtics de la època. Entre ells, es trobava **Alan Turing** (Il·lustració 15), matemàtic i criptòleg britànic, i considerat un dels pares de la computació, i precursor de la informàtica moderna.

Il·lustració 15: Alan Turing

Turing liderava l'equip de matemàtics britànics i polacs, i la seva tasca es va basar en intentar crear una rèplica de la màquina **Enigma**. Partint de la idea de **Rejewski**, es va donar lloc a noves màquines que intentaven verificar totes les possibles combinacions, que descartaven, quan es trobava una contradicció, grans quantitats de claus candidates, l'anomenada **Bomba de Turing**. De totes formes, era impossible fer les comprovacions de totes les combinacions en un temps raonable. Per això era molt important descartar combinacions errònies, extraient informació dels missatges enviats. Un dels avenços més grans fou la constatació que la **Enigma** mai podia codificar un caràcter com a sí mateix. Aquest fet aparentment simple, reduïa àmpliament les possibilitats de combinació.

El 9 de Maig del 1941, fou capturat un submarí alemany, aconseguint una màquina **Enigma** i el preuat **llibre de claus**. Aquesta captura es va mantenir en secret, deixant creure als alemanys que la nau s'havia enfonsat, aconseguint així que no canviessin els codis, i atorgant als aliats una gran avantatge sobre els nazis.

Durant els darrers anys de la Guerra, **Turing** va col·laborar en la creació de **Colossus**, una màquina totalment electrònica, i primer dispositiu calculador digital de la història i que ell mateix va considerar com un cervell primitiu. **Colossus** va tenir una gran importància en el desenllaç de la Guerra. Gràcies a aquesta màquina, al 1944 es van desxifrar comunicacions de l'exercit alemany, en les quals es mostraven convençuts que la invasió aliada tindria lloc a l'Estret de Calais. Coneguda aquesta creença, els exercits aliats finalment desembarcaren a Normandia, a 249 kilòmetres de Calais. En el moment en que Hitler va voler mobilitzar les divisions cuirassades, ja era massa tard. Les tropes aliades s'havien endinsat massa profundament a França. S'especula, doncs, que gràcies a la possibilitat de desxifrar els missatges de l'enemic per part de les tropes aliades, es va avançar el final de la guerra al menys **2 anys**.

2.2.2.3 Claude E. Shannon

Il·lustració 16: Claude E. Shannon

Claude Elwood Shannon (Il·lustració 16) va néixer al 1916 a Petoskey, Michigan, Estats Units. Des de molt jove va destacar per les seves inquietuds investigadores, i per l'habilitat per a crear prototipus tècnics.

Graduat a la Universitat de Michigan als 20 anys, va entrar a treballar al MIT com a ajudant d'investigació, i als 24 anys, presentava la seva tesi doctoral en matemàtiques sobre l'aplicació de l'àlgebra booleana en l'anàlisi de dades.

Al MIT es va ocupar del desenvolupament dels primers ordinadors, ben a prop de Vannevar Bush, creador de Memex, considerat l'antecedent d'internet.

La seva obra i aportació en diferents camps de les matemàtiques, enginyeria o intel·ligència artificial fou enorme. Però cal destacar per sobre de totes elles, la que ha estat qualificada com a carta magna de la era de la informació, la seva "**Teoria matemàtica de la comunicació**", obra enriquida posteriorment per Warren Weaver i publicada per la Universitat de de Illinois. En aquesta obra es detallaven les lleis que regien la transmissió i el processament de la informació. Més concretament, la mesura de la informació i de la representació de la mateixa (codificació), i de la capacitat dels sistemes de comunicació per transmetre-la i processar-la.

Va demostrar que **qualsevol font d'informació**, des dels aparells més sofisticats de l'època, com el telègraf, el telèfon o la radio, fins a quelcom tan familiar com una persona parlant, **es podien mesurar**, i que els canals de comunicació tenen una unitat de mesura similar. També va demostrar que la informació es pot transmetre sobre un canal, si i només si, la magnitud de la font no excedeix la capacitat del canal que la condueix. Assentà, igualment, les bases de la correcció d'errors i de la supressió de soroll i redundància. Es pot dir que aquesta obra és la base de tota la comunicació digital, que tan important ha esdevingut en els darrers anys.

A nivell criptogràfic, **Shannon** va introduir a la "**Teoria matemàtica de la comunicació**" dos conceptes molt importants:

- La **confusió** és la propietat per la qual la relació entre el text xifrat i la clau ha de ser tan complexa com sigui possible. És a dir, que si algú interceptés un missatge en clar, no pogués predir com es codificaria un caràcter d'aquest missatge al text xifrat.
- La **difusió** és la propietat per la qual, al canviar un bit del missatge en clar, s'haurien de canviar la major quantitat possible de bits al missatge xifrat. És a dir, que s'ha d'estendre la informació del text original a la totalitat del text xifrat, fent que els canvis al missatge es reflecteixin a moltes parts del text xifrat.

Per aquestes raons, **Claude E. Shannon** va rebre nombroses condecoracions i reconeixements de diverses universitats i institucions d'arreu del món, i tot i ser desconegut per al gran públic, ha de ser considerat com un dels personatges més importants del segle XX.

Claude E. Shannon va morir el 24 de Febrer del 2001 a Medford, Massachusetts, als 84 anys, després d'una llarga lluita contra la malaltia d'Alzheimer.

2.2.2.4 DES

Al Maig de 1973, i durant el mandat de Richard Nixon als Estats Units, la **National Bureau of Standards** (**NBS**, en les seves sigles en anglès, oficina nacional d'estàndards) va publicar una sol·licitud de propostes per a algoritmes criptogràfics per a protegir la transmissió i emmagatzemament de dades.

Inicialment no hi va haver respostes, fins que a l'Agost del 74, **IBM** va entregar el seu algoritme candidat. Conegut internament a IBM com a "**Lucifer**", fou avaluat i, amb una modificació, acceptat per la NBS com a nou estàndard per a l'encriptació de dades.

Lucifer era originàriament un algoritme de clau simètrica que treballava amb blocs de 128 bits, tenint una clau de la mateixa longitud. Es basava en operacions lògiques booleanes i es podia implementar de forma fàcil tant a nivell hardware com software. Estava destinat a ser un paquet comercial. La NBS, preocupada per haver d'examinar un paquet comercial que superava la seva capacitat d'anàlisi, va negociar amb IBM reduir la mida dels blocs i la clau a 64 bits, dels quals 8 són de paritat (per tant, realment la clau és de 56 bits). Per tant, es pot considerar **DES** com una **versió debilitada de Lucifer**. Això unit a la classificació com a secret de certs detalls de la selecció de fórmules, va generar molta controvèrsia. S'ha especulat amb l'existència de portes posteriors, que permetrien que el govern fos capaç de desxifrar els missatges.

Després de que diverses universitats, com Stanford, i companyies com Bell Telephone ataquessin la decisió de prendre DES com a estàndard, donada la manca de robustesa, el Comité d'Intel·ligència del Senat va investigar el cas. Sospitosament, no va trobar motius per a exigir una millora de l'algoritme.

El funcionament del **DES** consta de 19 etapes. La primera és una transposició, una permutació inicial del text pla de 64 bits, de forma independent de la clau. Després hi ha 16 etapes, que són una xarxa de Feistel de 16 rondes. Durant aquestes 16 rondes, s'empra un valor k_i obtingut a partir de la clau de 56 bits, i que és diferent a cadascuna de les 16 iteracions. La penúltima etapa intercanvia els 32 bits de l'esquerra i els 32 de la dreta. Finalment, a la darrera etapa, es fa una nova transposició del text, exactament la inversa de la realitzada a la primera ronda.

L'algoritme DES va resoldre, doncs, el problema de la estandardització, i va fer que inclús empreses del sector privat comencessin a emprar la criptografia com a mesura de seguretat. Al 1979, per exemple, el mercat de banca privada va començar a emprar DES per a codificar el PIN als caixers automàtics. Però tot i aconseguir un estàndard, i a pesar de la robustesa de DES com a mètode de xifrat, continuava existint un greu problema, la distribució de les claus secretes.

Es pot veure, de forma resumida, el funcionament de l'algoritme DES a l'Apèndix sobre el funcionament de l'algoritme DES.

2.2.2.5 Procediments de clau simètrica moderns

Posteriorment a l'aparició de l'algoritme **DES**, han aparegut molts altres algoritmes d'encriptació de clau simètrica, és a dir, algoritmes que comparteixen una mateixa clau tant l'emissor com el receptor per tal de xifrar i desxifrar els missatges. Entre els més destacats trobem els anomenats **Rivest Cypher**, (també coneguts com a Ron's Code) i denotats habitualment amb les sigles **RC**. Aquests són una sèrie de criptosistemes inventats pel criptògraf i professor de ciències de la computació al Massachusetts Institute of Technology (MIT) **Ronald Rivest** (Schenactady, New York, 1947). És conegut per ser el creador, juntament amb Adi Shamir i Leonard M. Adleman, del criptosistema de clau pública RSA, del que parlarem més endavant en aquest document, i dels algoritmes de Hash MD-2, MD-4 i MD-5.

Ronald Rivest és el creador dels RC des del 1 fins al 5, i és coautor, juntament amb Matt Robshaw, Ray Sidney i Yiqun Lisa Yin del **RC-6**, tot i que cal destacar que tant el RC-1 com el RC-3 mai no van arribar a ser publicats.

El criptosistema **RC-2** fou desenvolupat l'any 1989 per a la **RSA Data Security Inc**. És un algoritme de xifrat per blocs amb clau de mida variable, i que és entre 2 i 3 vegades més ràpid que el **DES**, i també més segur, tot i que, degut a un error de concepte, és considerat vulnerable a un atac de força bruta si la mida de claus és insuficient. Al 1994, es va fer públic el **RC-4**, també creat per a la RSA Data Security Inc. tot i que realment va ser dissenyat a l'any 1987. Aquest criptosistema és considerat immune al criptoanàlisi diferencial i lineal, i va ser emprat en el xifratge de xarxes inalàmbriques **WEP**. Aquest tipus de xifratge és considerat molt vulnerable, però s'ha de remarcar que no és degut a problemes amb l'algoritme **RC-4**, si no a altres aspectes del propi protocol **WEP**, que permeten determinar la clau en relativament poc temps si el tràfic de la xarxa és suficient.

També a l'any 1994 es publica el **RC-5**, que, com els anteriors, és un algoritme de xifrat per blocs de mida variable, de 32, 64 o 128 bits, amb una mida de clau que se situa entre 1 i 2040 bits. A més, el nombre de voltes o rondes a realitzar a l'algoritme estarà entre 1 i 255. La principal característica del **RC-5** és la seva senzillesa, cosa que el fa fàcilment implementable tant en hardware com en software.

A part dels RC, hi ha altres algoritmes de clau simètrica molt coneguts. Per exemple, a l'any 1991, i abans dels **RC-4** i **RC-5**, va aparèixer el criptosistema **IDEA**. Descrit pels professors de l'Escola Politècnica Federal de Zurich, Suïssa, **Xuejia Lai i James L. Massey**, va ser una de les propostes per a substituir al **DES** com a estàndard de criptografia. És un algoritme lliure i d'ús no comercial, ja que, tot i que en un principi va ser patentat, aquestes patents ja han vençut. L'**IDEA** va ser emprat a les primeres versions del **Pretty Good Privacy** (programa desenvolupat per **Phil Zimmermann** amb la finalitat de protegir la informació distribuïda a través d'internet), i és un algoritme que empra pel seu funcionament blocs de 64 bits, una clau de 128 bits i consisteix en 8 transformacions idèntiques, i una transformació de sortida final. El procés de xifrat i desxifrat és similar, i per al procés utilitza operacions amb grups de 16 bits del tipus OR-Exclusiva (XOR), suma de mòdul 2^{16} , i multiplicació $2^{16}+1$ on la paraula nul·la 0x0000 s'interpreta com a 2^{16} .

No es pot atacar l'**IDEA** per la força bruta, ja que el nombre de claus 10^{38} el fan impracticable amb el mitjans computacionals que existeixen actualment. A més, i sota certs criteris és immune a l'anàlisi diferencial, i no s'han descrit febleses en l'anàlisi lineal. Per tot això se'l considera un dels sistemes de xifrat en blocs més segurs que existeixen.

Un altre sistema de xifrat, el **Triple-DES** va ser desenvolupat a l'any 1998, degut a la manca de robustesa que començava a mostrar el **DES** i la seva clau de 56 bits. Una clau tan curta el feia vulnerable a un atac per força bruta, degut als avenços en matèria computacional que s'estan produint darrerament, i que fan que tasques que es consideraven inabastables fins no fa masses anys, ara puguin ser dutes a terme en un període de temps no molt elevat.

El **Triple-DES** va ser desenvolupat per IBM, i el seu funcionament es basa en realitzar tres cops el xifrat **DES**. Fou triat como una manera d'ampliar la llargada de la clau d'encriptació sense alterar l'algoritme de xifrat original. **Triple-DES** dobla la longitud efectiva de la clau de xifrat, però no triplica la quantitat d'operacions a realitzar. La variable més simple funciona segons aquesta fórmula:

$$C = E_{DES}^{k3}(D_{DES}^{k2}(E_{DES}^{k1}(M)))$$

M és el missatge en clar, C el missatge xifrat, i k_1 , k_2 i k_3 són les claus de xifratge del **DES**.

L'any 1997, el **NIST** (National Institute of Standards and Technology, abans conegut com a NBS, National Bereau of Standards) va convocar un concurs mitjançant el qual, volia escollir un algoritme de xifrat capaç de protegir la informació important al segle XXI. Aquest algoritme s'anomenaria **AES** (**Advanced Encryption Standard**). A l'agost del 1999, el **NIST** va decidir els cinc finalistes:

- **Mars** (IBM).
- **RC-6** (Ronald Rivest, Matt Robshaw, Ray Sidney i Yiqun Lisa Yin per als RSA Laboratories).
- **Rijndael** (John Daemen, Vincent Rijmen).
- **Serpent** (Ross Anderson, Eli Biham, Lars Knudsen).
- **Twofish** (Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, Niels Ferguson).

Finalment, l'algoritme que va resultar escollit a l'any 2001 fou el **Rijndael**, substituint al **DES** com a estàndard de xifrat de les comunicacions del govern dels Estats Units. Aquest algoritme va ser dissenyat pels dos criptòlegs belgues **Joan Daemen** i **Vincent Rijmen**, estudiants de la Katholieke Universiteit Leuven, a Lovaine, Bèlgica. Aquest és un algoritme de blocs, en el qual la mida del bloc i de la clau són variables. A l'estàndard s'adopten blocs de 128 bits, i una clau de 128 (l'algoritme emprarà 10 rondes per a l'encriptació), 192 (12 rondes per a l'encriptació) o 256 bits (14 rondes per al procés d'encriptació). És un dels algoritmes més estesos, i possiblement, degut al fet de ser l'estàndard, un dels més analitzats del món. Fins al moment ha demostrat una enorme robustesa.

El bucle principal de l'algoritme Rijndael (AES) empra les següents funcions en el següent ordre:

1. SubBytes() - Barreja de cadascun dels bytes.
2. ShiftRows() - Barreja de cadascuna de les files.
3. MixColumns() - Barreja de cadascuna de les columnes.
4. AddRoundKey() - Encriptació.

Les 3 primeres funcions del AES estan dissenyades per frustrar el criptoanàlisi a través de la confusió i la difusió. La quarta funció és l'encarregada de la encriptació real.

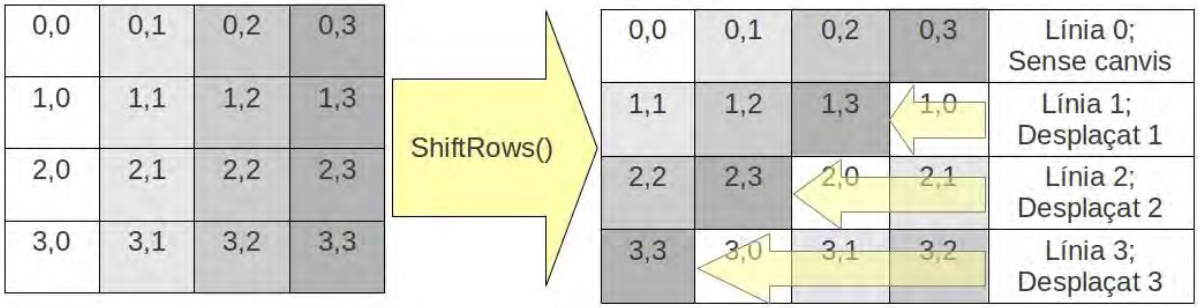
Primerament, l'AES formateja el text original en blocs de 16 bytes (128 bits), i tracta cadascun dels blocs com una taula de 4x4. Aquesta taula serà la que contindrà la informació de files i columnes que s'emprarà a les funcions prèviament esmentades. Les 4 funcions seran aplicades en les n-rondes que ens marqui la longitud de la clau d'encriptació (128 bits – 10 rondes, 192 bits – 12 rondes, 256 bits – 14 rondes).

La funció de SubBytes() afegeix confusió processant cada byte a través de les anomenades S-Caixes (S-Boxes). Cada S-Caixa és una taula de substitució que reemplaça cada byte per un altre, basant-se en un algoritme de substitució.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3B	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

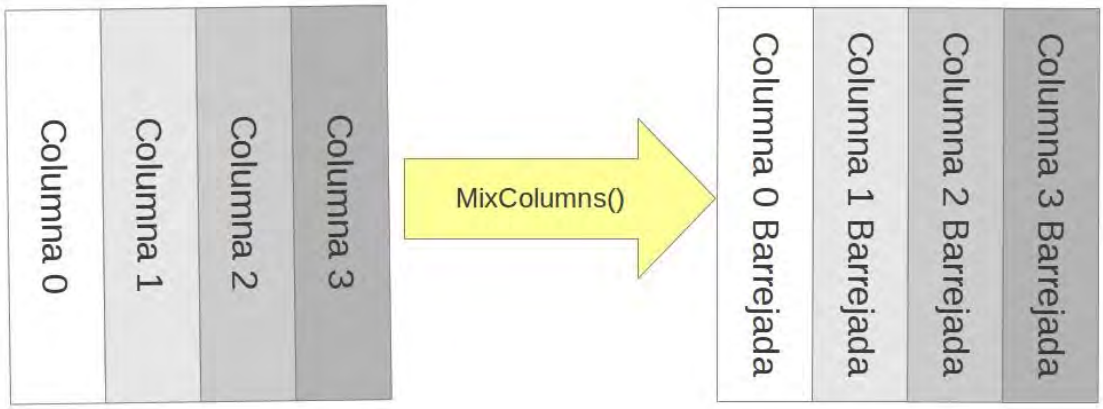
Per exemple, si la cadena que volem encriptar és “ABC” prenem els valors hexadecimals de cada byte. El codi ASCII de “A” hexadecimal serà 0x42, el de “B” serà 0x43 i el de “C” serà 0x44. Agafant el primer digit hexadecimal com la fila de la taula i el segon com la columna, “A”=0x42 passa a ser 0x2C, “B”=0x43 passa a 0x1A i “C”=0x44 passa a 0x1B.

La funció ShiftRows() (Il·lustració 17)proveeix difusió al sistema, barrejant la informació a dins de les línies. La línia 0 no es modifica, la 1 es desplaça un byte a l'esquerra, la línia 2, 2 bytes a l'esquerra, i així successivament.



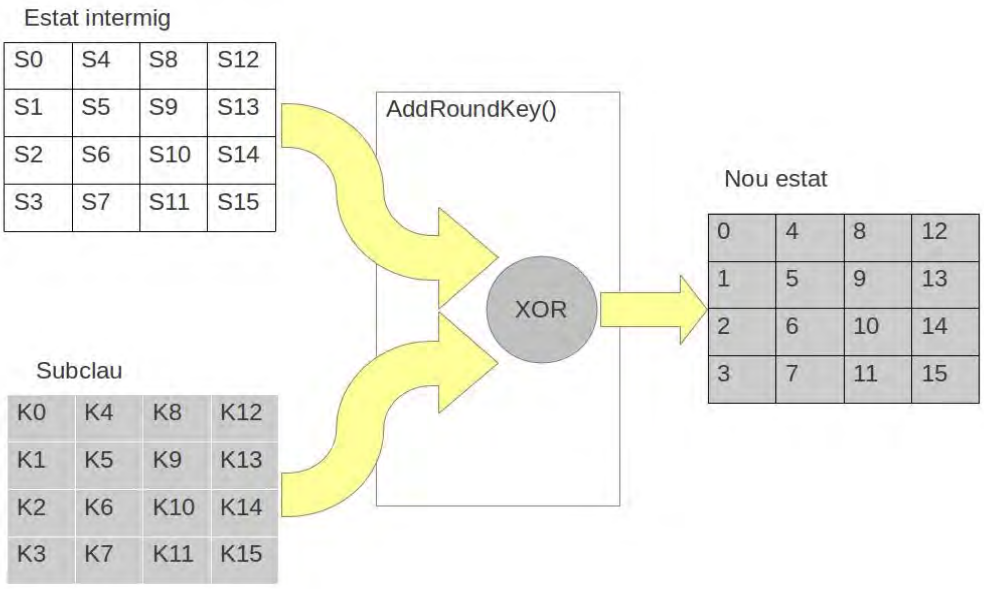
Il·lustració 17: Funció ShiftRows() AES

La funció MixColumns() (Il·lustració 18) també afegeix difusió però aquest cop barrejant la informació entre les columnes. El 4 bytes que formen cada columna es tracten com un número de 4 bytes, que es transformat en un altre número mitjançant camps finits matemàtics.



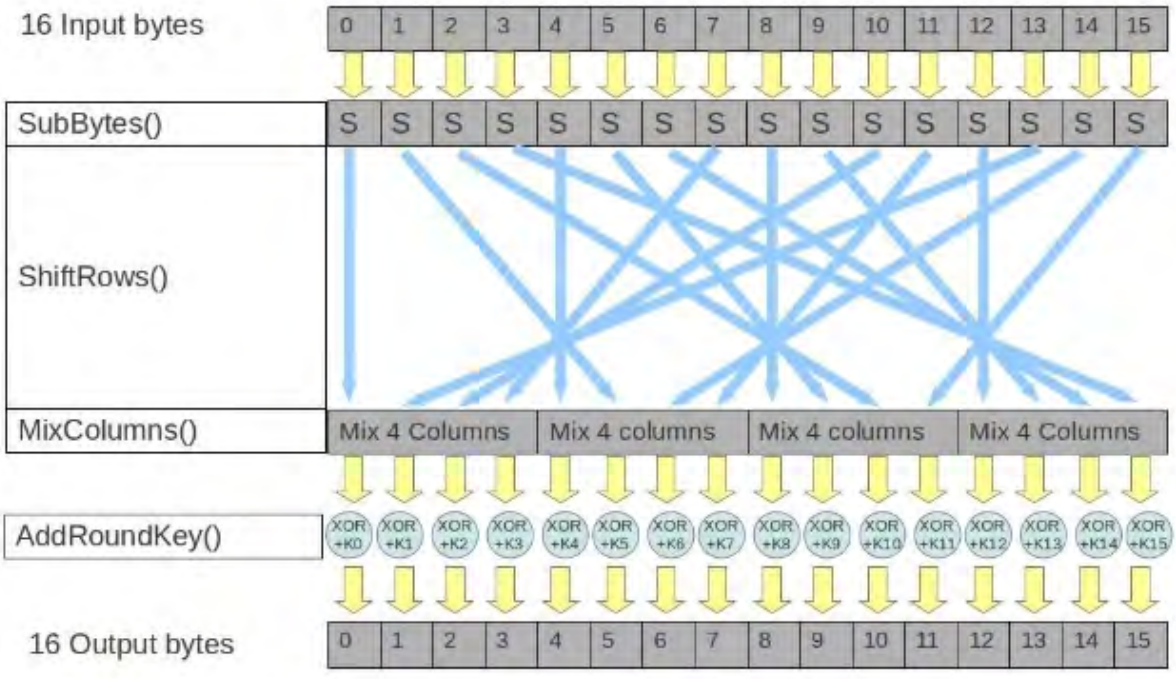
Il·lustració 18: Funcio MixColumns() AES

La funció AddRoundKey() (Il·lustració 19) serà l'encarregada d'encriptar, aplicant a cada byte dels resultats intermedis una operació XOR juntament amb la subclau. La subclau serà derivada de la clau mitjançant una tècnica d'expansió.



Il·lustració 19: Funció AddRoundKey() AES

Per desencriptar es fa servir la mateixa funció AddRoundKey(), i la inversa de les funcions ShiftRows(), SubBytes() i MixColumns(). La funció AddRoundKey() no requereix d'inversa, perquè l'operació XOR ens retornarà l'entrada original al ser aplicada dues vegades amb la subclau corresponent (Il·lustració 20).



Il·lustració 20: Una Ronda del AES

2.3 Criptografia asimètrica o de clau pública

Tots els sistemes de xifrat dels que s'ha parlat fins ara, són **sistemes** anomenats **simètrics**. Això significa que tant l'emissor com el receptor utilitzen la **mateixa clau d'encriptació**, i que els dos l'han de mantenir en **secret**. Un dels més greus problemes d'aquests sistemes sempre havia estat l'**intercanvi de claus** a través del que s'ha donat a anomenar un 'canal segur'. Des del simple contacte cara a cara entre els interlocutors fins al preuat llibre de claus de la Enigma, passant pels missatgers de confiança, aquest era una sistema difícil de mantenir, especialment quan s'incrementava el nombre de participants en la comunicació (la clau és coneguda per moltes persones, i és molt difícil de controlar que tothom tingui la cura necessària de mantenir la clau en secret), o es modificaven les claus de xifrat sovint (una pràctica que és molt recomanable per millorar la seguretat a les comunicacions, donat que es disposa d'un temps finit per a l'anàlisi de la comunicació). Si a tot plegat afegim la possibilitat de fer que les comunicacions siguin segures a davant d'altres usuaris del mateix sistema, es fa necessari l'ús d'una clau específica diferent per cada parell d'interlocutors.

L'intent d'evitar tots aquests problemes generats per l'ús de claus privades va fer sorgir als anys 70 un nou tipus de criptosistemes que van suposar una revolució al món de la criptografia. Els **sistemes asimètrics o de clau pública**. Aquests es caracteritzen per utilitzar un parell de claus relacionades matemàticament en els quals una desxifra allò que s'ha xifrat amb l'altra. D'aquesta manera, cada usuari només necessita un parell de claus, de les quals només una d'elles serà **privada (secreta)**. L'altra serà una **clau pública**, i pel seu intercanvi no és necessari cap canal segur, donat que aquesta clau pot ser visible per a qualsevol, sense comprometre la seguretat del sistema, i aconseguint així que aquest parell de claus puguin ser utilitzades de forma indefinida.

Aquests algoritmes es basen en problemes matemàtics anomenats '**funcions d'un sol sentit**'. Aquests problemes tenen la característica de ser fàcils de calcular, implicant un cost computacional molt baix. Però el càlcul de la seva inversa implica un cost computacional extremadament elevat. Entre aquest problemes el més típic és el càlcul de la multiplicació de dos nombres primers. La seva multiplicació és un problema bastant simple, però factoritzar el resultat d'aquesta operació és un procés molt complicat quan ens referim a nombres primers elevats.

El problema de les funcions d'un sol sentit, és que necessiten **claus generalment llargues** per aconseguir una bona robustesa, i moltes claus candidates de curta llargada són rebutjades ràpidament, degut a la inseguretat que provocarien. En l'exemple de la multiplicació de nombres primers, si els nombres fossin molt petits, factoritzar-los, no tindria un cost computacional relatiu tan elevat, exposant el sistema a atacs que tindrien èxit molt ràpidament. El fet d'haver de generar el parell de claus adient, i el propi procés de xifrat i desxifrat dels missatges, fa que aquests criptosistemes tinguin un cost computacional elevat. En canvi, els sistemes de clau simètrica poden donar la mateixa robustesa amb claus molt més curtes, i generalment poden ser inclús series seudoaleatòries de bits, fàcils de generar, i que poden ser utilitzades a molt curt plaç, inclús per a un únic ús. Per tant, a la pràctica, se sol utilitzar un algoritme de clau pública amb una clau suficientment llarga únicament per a l'intercanvi de la clau simètrica d'un sol ús, que serà molt més curta però igual de forta. S'aconsegueix així fer anar l'algoritme de clau pública, que és molt més lent, només a l'inici de la comunicació, i per a la resta de la conversa, es fa anar l'algoritme de clau simètrica, que és molt més ràpid.

Fins ara, l'intercanvi de claus de **Diffie-Hellman** i el famós algoritme **RSA**, anomenat així per les inicials dels seus creadors, **Ronald R. Rivest, Adi Shamir i Leonard M. Adleman**, havien estat considerats com els precursors dels sistemes de clau pública. Cal assenyalar, però, que darrerament

s'han publicat uns escrits per part del govern britànic, segons els quals el **GCHQ (Goverment Communications Headquarters)** de Cheltenham, la institució d'alt secret britànica formada de les restes de Bletchley Park després de la Segona Guerra Mundial, van ser els creadors de la criptografia de clau pública. Aquest documents classificats indicarien que durant els anys 60 i 70, van crear uns criptosistemes en essència idèntics al **RSA** i a l'intercanvi de claus de **Diffie-Hellman**. Alguns dels seus inventors, com **James H. Ellis, Clifford Cocks** o **Malcom Willamson** han fet públic ara part del seu treball d'aleshores.

2.3.1 Diffie-Hellman

A l'any 1976, els criptògrafs estatunidencs **Bailey Whitfield "Whit" Diffie** (5 de Juny de 1944) i **Martin Edward Hellman** (2 d'Octubre del 1945) van publicar el seu "**New Directions in Criptography**", introduint un canvi radical a la ciència criptogràfica. Van idear un mètode de distribució de claus que va solucionar un dels més greus problemes de la criptografia. Conegut com a protocol **Diffie-Hellman**, va donar pas a un nou tipus d'algoritmes d'encriptació coneguts com a algoritmes de clau asimètrica.

Aquest protocol dóna la capacitat d'acordar una clau secreta de comunicació entre dues màquines, a través d'un canal insegur, i fent servir només dos missatges. La clau secreta que en resulta no pot ser descoberta per un atacant, **ni tan sols interceptant els dos missatges** enviats pel protocol. D'aquesta manera, la principal aplicació és acordar una clau simètrica amb que xifrar les comunicacions entre les dues màquines.

Actualment, se sap que aquest protocol és sensible a atacs actius de tipus **Man-in-the-middle**. Si un atacant se situa enmig de les dues màquines que es comuniquen, es pot fer passar per emissor de cadascun dels destinataris, ja que no es disposa de mecanismes de validació de la identitat dels participants a la comunicació. Així, acordaria una clau simètrica per a cada una de les parts i retransmetria les dades entre ells, escoltant la conversa en ambdós sentits. Un cop establertes les dues claus simètriques, l'atacant podria fer de pont entre els dos comunicadors, desxifrant tota la informació, i tornant a xifrar-la per ser retransmesa al host de destí, i que els comunicadors no s'adonin de l'atac. Per tal de corregir aquesta vulnerabilitat, el protocol **Diffie-Hellman** se sol fer anar conjuntament amb tècniques de control de temps, autenticació de les parts, o bé autenticació del contingut.

Farem un exemple del protocol **Diffie-Hellman**, en el que dos comunicadors, **A** i **B** establiran una clau secreta de comunicació. La implementació inclou un nombre primer **p**, i una base **g**. Per exemple, **p**=23 i **g**=5.

A tria un nombre secret a tal que (**a**<**p**), per exemple **a**=6. **B** tria un nombre secret **b** tal que (**b**<**p**), per exemple **b**=15.

A envia $(g^a \bmod p) = (5^6 \bmod 23) = 8$

B envia $(g^b \bmod p) = (5^{15} \bmod 26) = 19$

Per tal de generar la clau secreta, **A** ha de calcular $(g^b \bmod p)^a = (5^{15} \bmod 23)^6 = 2$.

Per tal de generar la clau secreta, **B** ha de calcular $(g^a \bmod p)^b = (5^6 \bmod 23)^{15} = 2$.

Per tant, la clau secreta serà $(5^{15} \bmod 23)^6 = (5^6 \bmod 23)^{15} = 2$.

Els valors de **p** i **g** són públics, i qualsevol atacant els pot conèixer, però això no suposa una vulnerabilitat. Tot i que un atacant conegui els aquests valors, i capturi els dos missatges enviats entre **A** i **B**, seria incapaç d'esbrinar la clau secreta. Els missatges que capturaria serien

$(g^a \bmod p) = (5^6 \bmod 23) = 8$
$(g^b \bmod p) = (5^{15} \bmod 26) = 19$

A partir de les equacions capturades, intentar calcular els valors de **a** i **b** és el que es coneix com

el problema de l'algoritme discret, un problema que es creu computacionalment intractable:

$$a = \log disc_g(g^a \bmod p) = \log disc_5(8)$$

$$b = \log disc_g(g^b \bmod p) = \log disc_5(19)$$

Amb aquests valors, és possible trobar la solució, perquè el nombre primer **p** és molt petit (p=23), i és conegut que **a** i **b** són menors que **p**. Per tant, per obtenir els valors secrets, l'atacant només hauria de provar 22 possibles valors.

És per aquest motiu que les implementacions més actuals de Diffie-Hellman empren nombres primers molt grans, cosa que fa impossible a un atacant calcular els valors **a** i **b**. El valor g no necessita ser gran, i a la pràctica el seu valor és 2 o 5. Al RFC 3526 (Request For Comments, propostes oficials per a estàndards per a protocols d'internet) apareixen publicats els nombres primers que s'han d'utilitzar. Com a exemple, es facilita aquí el nombre primer de 1024 bytes proposat. El valor **g** emprat és 2:

$$p = 2^{8192} - 2^{8128} - 1 + 2^{64} \cdot ((2^{8062} pi) + 4743158)$$

2.3.2 RSA

El sistema **RSA** deu el seu nom a les inicials dels professors del MIT (Massachusetts Institute of Technology) **Ronald r. Rivest, Adi Shamir** i **Leonard M. Adleman**, que el van dissenyar a l'any 1977.

Aquest és un sistema de clau pública, per tant, cada usuari tindrà dos claus de xifrat, una pública i una privada. Per encriptar un missatge, l'emissor utilitzarà la clau pública del receptor. Un cop el missatge xifrat ja és a mans del destinatari, aquest només ha d'utilitzar la seva clau privada per desencriptar el contingut.

L'**RSA** es basa en el problema matemàtic de la **factorització de nombres sencers**, concretament en la factorització del producte de dos nombres primers grans. És molt fàcil saber si un nombre és primer, però és extremadament complicat factoritzar en nombres primers un nombre sencer molt elevat, no per la dificultat dels algoritmes existents per aquest càlcul, si no pel consum de recursos físics (memòria, necessitats hardware, inclús temps d'execució...) necessaris per dur a terme aquests algoritmes. S'ha demostrat que si 'n' és el nombre de dígits binaris de la entrada de qualsevol algoritme de factorització, el seu cost serà $\theta(2n)$. Això vol dir que el seu temps d'execució serà molt elevat, pertanyent a la categoria dels anomenats **problemes intractables**. Actualment els nombres primers emprats són de l'ordre de 10^{200} , però es preveu que amb l'augment de capacitat computacional dels ordinadors, aquesta mesura creixi en consonància.

El funcionament del **RSA** consta de tres passos. Primerament s'ha de calcular el parell de claus pública i privada que s'utilitzaran per xifrar i desxifrar. Per fer-ho, es segueixen els següents passos:

1. Es trien dos nombres primers grans, com a mínim de l'ordre de 100 dígits, anomenats **p** i **q**. Per motius de seguretat, aquests nombres haurien de ser triats de forma aleatòria, i tenir els dos una longitud de bits similar. Es pot emprar el test de primalitat per escollir-los.
2. S'ha de calcular **n**=**p**·**q**, que serà utilitzat com el mòdul per a les dues claus, tant la pública com la privada.
3. S'ha de calcular $\varphi(n)=(p-1)\cdot(q-1)$ a on φ és la funció d'Euler.
4. S'ha de triar un nombre sencer positiu **e** < $\varphi(n)$, i que sigui coprimer amb $\varphi(n)$. **e** serà anomenat exponent de la clau pública. Si **e** és triat amb una suma encadenada curta, el xifrat serà més efectiu. Un exponent **e** molt petit, podria suposar un risc de seguretat en aquest criptosistema.
5. S'ha de determinar **d** que compleixi que $d=e^{-1} mod\, \varphi(n)$, o el que és el mateix, que **d** sigui l'invers modular de la multiplicació de $e mod\, \varphi(n)$. Per realitzar aquest càlcul, se sol emprar l'algoritme d'Euclides estès. **d** serà l'exponent de la clau privada.

La clau pública serà (n,e), on **n** és el mòdul, i **e** l'exponent de xifrat. La clau privada serà (n,d) on **n** és el mòdul, i **d** l'exponent de xifrat. Aquesta és la clau que ha de mantenir-se en secret.

Posarem un exemple del criptosistema **RSA**:

- El primer pas serà la generació de claus. Triarem dos nombres primers **p** i **q**.

  P=101, q=113 => n=p·q=11413 $\varphi(n)=(p-1)\cdot(q-1)=100\cdot112=11200$

- Triem **e** (exponent de desencriptació) que ha de ser coprimer amb **n**, és a dir, el seu màxim comú denominador ha de ser 1. Un possible **e** serà **e**=6597.

- Calculem l'invers modular de **d** emprant l'algoritme d'Euclides, és a dir, $e \cdot d = 1 \, mod \, \varphi(n)$

  Per tant, **d**=3533.

  Clau Pública=(d,n) Clau Privada=(e,n)

- Encriptació: $E_k(m) = m^d \, mod \, (n)$

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Si el missatge a enviar fos, per exemple, '**OPERACIO**':

M = **OPERACIO** = **151651813915**

Dividint el missatge en blocs de mida màxima n-1 (nosaltres prenem 4).

$m_1 = 1516 \rightarrow c_1 = 1516^{3533} \, mod \, 11413 = 5556$

$m_2 = 5181 \rightarrow c_2 = 5181^{3533} \, mod \, 11413 = 7771$

$m_3 = 3915 \rightarrow c_3 = 3915^{3533} \, mod \, 11413 = 1434$

- Desencriptació $D_k(c) = c^e \, mod \, (n)$

$c_1 = 5556 \rightarrow m_1 = 5556^{6597} \, mod \, 11413 = 1516$

$c_2 = 7771 \rightarrow m_2 = 7771^{6597} \, mod \, 11413 = 5181$

$c_3 = 1434 \rightarrow m_3 = 1434^{3533} \, mod \, 11413 = 3915$

D'aquesta forma, el missatge en clar serà **151651813915** = '**OPERACIO**'

2.3.3 ElGamal

Aquest és un algoritme de clau pública emprat en software **GNU Privacy Guard**, versions recents del **Pretty Good Privacy**, i altres sistemes criptogràfics. És un sistema d'ús lliure, degut a que no està sotmès a cap patent. Entre els anys 1984 i 1985,el criptògraf egipci **Taher Elgamal** va descriure i desenvolupar aquest criptosistema basant-se en el problema matemàtic del logaritme discret sobre un grup multiplicatiu d'un cos finit. Aquest és un problema intractable computacionalment. Tot i que no se sol utilitzar de forma directa, perquè la seva velocitat de xifrat i autenticació és inferior a la del **RSA**, i produeix signatures més llargues (de l'ordre del doble de mida que el text original), l'algoritme de **ElGamal** té molta importància per al desenvolupament del **Digital Signature Standard** (**DSS**), l'estàndard de signatura digital del National Institute of Standards and Technology (NIST) del Estats Units. La característica que el fa diferent de la resta de criptosistemes de clau pública és que en el procés de xifrat, no només es fa servir la clau pública, si no també la clau privada de l'emissor.

El funcionament d'aquest algoritme, també consta de tres passos, la creació de les claus de xifrat, l'algoritme de xifrat i el de desxifrat. Seguidament veurem un exemple d'aquest algoritme emprant el grup multiplicactiu de sencers mòdul **p**.

Per crear un parell de claus, primerament s'ha de triar un nombre primer **p** qualsevol, tal que **p-1** tingui un factor primer gran. Es trien a continuació dos nombres aleatoris **g** (el generador) i **a** (que serà la clau privada), tal que a $a \in \{0,..., p-1\}$. S'ha de tenir en compte, però, que des d'un punt de vista de seguretat, aquesta definició té certs casos sense sentit, com són $g^0 = 1$ i $g^1 = g$ que no atorguen cap mena de seguretat, i fan que el xifrat no funcioni. Per tant, considerarem preferentment $a \in \{2,..., p-1\}$.

Calculem llavors el valor de $A = g^a (mod\ p)$. **A** serà la la clau pública.

El nombre a serà la clau privada, mentre que els valors **p**, **g** i **A** són públics.

Prenem, per exemple, els valors:

- p = 17 (triat aleatòriament).
- g = 3 (generador).
- a= 6 (clau privada triada aleatòriament).
- $A = g^a (mod\ p) = 3^6 (mod\ 17) = 15$ (clau pública).

Per tant la clau pública la formaran (17, 3, 15) i la privada serà (6).

Per tal de xifrar, el primer que s'ha de fer és convertir el text en un element de **G**, obtenint u **m**. Després s'agafa arbitràriament un nombre **b** tal que $b \in \{2,..., p-1\}$.

Calculem: $y_1 = g^b (mod\ p)$

$y_2 = A^b m (mod\ p)$

El missatge xifrat serà: $C_b(m,b) = (y_1, y_2)$

Continuant amb l'exemple numèric, si el missatge a transmetre és **m=9** i triem un **b=5** aleatori:

$y_1 = g^b (mod\ p) = 3^5 (mod\ 17) = 5$

$y_2 = A^b m \pmod p = 15^5 \cdot 9 \pmod{17} = 1$

El text xifrat serà $C_b(m,b) = (y_1, y_2) = (y_1 = 5, y_2 = 1)$

Per tal de desxifrar farem:

$y_1^x y_2 \pmod p$ on $x = p - 1 - a$

Per tant, resoldrem el problema utilitzant el Petit teorema de Fermat: $y_1^x y_2 = y_1^{p-1-a} y_2 = g^{b(p-1-a)} A^b m = (g^{p-1})^b (g^a)^{-b} A^b m = (A^{-b} A^b m) = m \pmod p$

A l'exemple:

$C_b(m,b) = (y_1 = 5, y_2 = 1)$ xifrat amb la clau pública $(p = 17, g = 3, A = 15)$ es pot desxifrar amb la clau privada $(a = 6)$.

Amb el Teorema Petit de Fermat:

$m = y_1^{p-1-a} y_2 \pmod p = 5^{10} \cdot 1 \pmod{17} = 9$.

2.3.4 Corbes el·líptiques

Fins ara havíem vist com els sistemes criptogràfics de clau pública basen la seva seguretat en l'ús de problemes de molt difícil resolució. Aquesta dificultat, i el fet que no existeixin algoritmes de resolució d'aquests problemes d'una forma ràpida i eficient, fan que els sistemes de computació actuals siguin incapaços de trencar els criptosistemes mitjançant **atacs de força bruta**, és a dir, provant totes les possibles solucions, en un temps raonable. Especialment si les claus triades per a l'encriptació són d'una mida considerable. El problema d'aquests sistemes de clau pública sempre ha estat que, per tal d'obtenir la mateixa seguretat que ens donen els sistemes simètrics, la **mida de les claus ha de ser molt més gran**, provocant que el cost computacional del propi xifrat sigui relativament elevat. A més, hem de tenir en compte que generar claus adients i de la mida necessària té també un cert cost.

A l'any 1985 i de forma independent, **Neal Koblitz**(professor de matemàtiques a la Universitat de Washington, nascut el 24 de Desembre de 1948) i **Victor S. Miller** (matemàtic al CCR, Center for Communications Research del Institute for Defense Analyses a Princeton, New Jersey, nascut el 3 de Març de 1947) van proposar la utilització de **corbes el·líptiques** com a mètode de xifrat de clau pública, argumentant major rapidesa, l'ús de claus més curtes que els sistemes criptogràfics de clau pública anteriors, com el **RSA**, però donant la mateixa robustesa i seguretat, i l'ampli ventall de grups que ofereix sobre el mateix cos base.

Fins ara, els criptosistemes de corbes el·líptiques no han estat molt utilitzats, però comencen a ser comuns, per exemple, en sistemes d'identificació mitjançant targetes, degut a la mida més reduïda que requereixen les seves claus, i que els fan idonis per a aquest tipus de tecnologies que necessiten uns requeriments de memòria i hardware relativament continguts.

Així com a l'algoritme **RSA** el problema consistia en la factorització de nombres, a la criptografia de corbes el·líptiques es tracta de l'obtenció de logaritmes. Si tenim una expressió del tipus

$$a^x = b \quad \text{, llavors} \quad x = \log(a)b$$

Trobar un logaritme no és molt més complicat que calcular una potència, així que per aconseguir que sigui un problema intractable, s'afegeixen una sèrie de condicions. En primer lloc, necessitem treballar a sobre d'un grup, és a dir, un conjunt d'elements units per una operació matemàtica. Anomenarem aquesta operació matemàtica (*). Aquesta operació ha de complir que:

- Si **a** i **b** són elements del grup, **a*b** també és element del grup.
- S'ha de complir la propietat associativa, és a dir, **a*(b*c) = (a*b)*c**.
- Ha d'existir un element neutre 1, tal que **a*1 = 1*a = a**.
- Ha d'existir l'element invers y, tal que **x*y = y*x = 1**.

Per exemple, el conjunt de nombres sencers amb la operació suma, i amb el 0 com a neutre, formaria el que hem comentat, un grup.

Dintre de tots els grups existents, els que ens interessen per al seu ús a les corbes el·líptiques són els grups cíclics, és a dir, aquells grups en els que tots els seus elements es poden obtenir mitjançant un de sol, anomenat generador. Si, a més, la operació aplicada és la multiplicació, es denominarà **Grup Cíclic Multiplicatiu**. Per exemple, tenim el grup que formen les 4 arrels quartes de 1: seran +1, -1, +i, -i (i és l'arrel quadrada de 1). Aquest i pot fer de multiplicador:

- i*(+1) = i.
- i*(+i) = -1.
- i*(-1) = -i.
- i*(-i) = 1.

L'operació de multiplicació ens permet complicar l'obtenció de logaritmes. Suposant un grup **G** amb **n** elements, i **b** un generador, podem obtenir tots els elements del grup com:

$$\{1, b, b^2, b^3, b^4, ..., b^{n-1}\}$$

Per tant, hi haurà un nombre **k**, tal que es pot escriure $g=b^k$ per a qualsevol nombre **g** que formi part del grup. En realitat existeixen molts possibles nombres k que compleixen aquesta propietat. Si, per exemple, prenem **k'=k+n** , podem comprovar que:

$$b^{k+n}=(b^k)*(b^n) \text{ , i } b^n=1$$

De la qual cosa es dedueix que, qualsevol parell de sencers **k**, **k'** capaços de representar l'element **g** són congruents mòdul **n**, és a dir, ens donen el mateix reste quan els dividim per **n**.

Si en lloc de referir-nos a tot el camp dels nombres reals, ens referim al grup cíclic **G**, el logaritme discret de **g** en base **b** és la operació inversa a la potència $g=b^k$, és a dir, $k=\log(b)\,g$.

En el cas del grup de les arrels quartes de 1 tindríem **b=i**, **k=0,1,2,3**.

- $b^k=g \quad \rightarrow \quad k=\log(b)\,g$.
- $i*1=i \quad \rightarrow \quad 1=\log(i)\,i$.
- $i*2=-1 \quad \rightarrow \quad 2=\log(i)(-1)$.
- $i*3=-i \quad \rightarrow \quad 3=\log(i)(-i)$.
- $i*4=1 \quad \rightarrow \quad 4=\log(i)(1)$.

En aquest grup, està clar que la dificultat del càlcul no serà molt elevada. Tenim només **n=4** elements, i donant un cop d'ull a la taula sabem ràpidament que el logaritme discret de cadascun dels elements. Per exemple, si volem saber el logaritme discret de **-i**, veurem que $i^3=-i$, i per tant la resposta serà **k=3**.

Però què passaria si, en lloc de **n=4**, fos, per exemple, de l'ordre de $n=2^{100}$? Calcular tots els $g, g^2, g^3, ..., g^{2^{100}}$ seria un greu problema, ens requeriria un temps d'execució polinòmic. Realitzar el càlcul $g=b^k$ és fàcil, però realitzar la seva inversa, és a dir, $k=\log(b)\,g$ és molt més complicat. En un atac per força bruta, el fet d'haver de comprovar totes les possibilitats fins a trobar quin **k** és el que ens ha permès generar **g** és un problema intractable amb els mitjans computacionals dels que es disposa avui en dia.

Si a l'algoritme de Diffie-Hellman el grup que ens permet crear el sistema de xifrat és **Zn* (grup multiplicatiu de sencer mòdul n)** als algoritmes de corbes el·líptiques el grup G serà creat de la següent manera. Prenem una corba denotada per la equació

$$y^2=x^3+ax+b$$

on **a** i **b** són nombres reals que compleixen $4a^3+27b^2\neq 0$.

Per a cada parell de valors **a** i **b**, la corba ens donarà un grup de possibles punts **(x,y)** que resolen l'equació. Aquests punts formaran un grup. Els nombres **x** i **y** són reals i formen un "**camp finit**" , però els punts (x,y) (formats per les "coordenades x i y), formen un grup, (es pot fer un símil amb les coordenades geogràfiques a un pla, podem tenir una longitud 8.1, i una latitud 34.7. Els nombres 8.1 i 34.7 són una cosa, però el punt geogràfic que representen n'és una altra).

L'esquema de funcionament d'un criptosistema de corbes el·líptiques seria així:

- Escollim una **corba el·líptica**.
- Aquesta corba que hem triat, té un **conjunt de solucions (x,y)**.
- Si els valors x i y pertanyen a un camp finit, llavors els punts (x,y) de la corba que representen formen un **grup**.
- Prenem un element del **grup**, i trobem el seu **logaritme discret** per a una base donada. Això ens servirà per establir algoritmes criptogràfics d'**intercanvi de claus** i de **signatura digital**.

El sistema de **corba el·líptica** és més complexe que el del **RSA**, no ha estat tant estudiat per tal de trobar-hi problemàtiques, i és molt més lent en la implementació inicial. Com a punts a favor trobem una mida de claus més curta, però tot i així, més llargues que els dels criptosistemes simètrics. Segons el NIST (National Institute of Standards and Technology) els sistema simètric **AES** amb una clau de 128 bits, proporciona la mateixa seguretat que els criptosistemes de corbes el·líptiques de 256 bits o la de l'algoritme asimètric **RSA** amb una clau de 3072bits.

Un altre dels inconvenients dels sistemes de corba el·líptica és que la major part de les variant d'aquests sistemes estan patentades, i no són d'ús lliure. La principal empresa que comercialitza aquestes tecnologies s'anomena **Certicom**, i posseeix unes 130 patents, atorgant llicències, per exemple, a la NSA(National Security Agency) americana per valor de 25 milions de dòlars. **Certicom** ha patrocinat diversos desafiaments al seu algoritme de corbes el·líptiques. El més complexe que s'ha resolt fins ara és el de clau de 109 bits. Un equip de la Universitat de Notre Dame, Indiana,va aconseguir, mitjançant un atac de força bruta, i fent servir més de 10000 ordinadors treballant 24 hores al dia, durant 549 dies, desxifrar el missatge del desafiament. La longitud de clau recomanada per als sistemes de corbes el·líptiques és de 163 bits, i es calcula que, amb els mateixos mitjans, es requeririen 100 milions de vegades més de temps que amb el repte de 109 bits, per tal de resoldre el problema.

Fins aquí aquesta breu repassada sobre la criptografia a la història. Existeixen molts altres mètodes d'encriptació, i sobretot, en els darrers anys, s'han creat molts altres criptosistemes que no han estat mencionats en aquestes breus notes. Però els que han estat descrits són alguns dels més remarcables, i que per diversos motius, han estat importants a la història d'aquesta disciplina.

2. 4 Signatura electrònica

2.4.1 Introducció

Qualsevol tècnica electrònica, informàtica i/o telemàtica, i que ens aporta les mateixes funcions que una firma de document escrita sobre paper, rep el nom de **signatura electrònica**. Aquest és un **concepte legal** mitjançant el qual, una persona accepta el contingut d'un missatge, a través de diversos mitjans electrònics vàlids.

Les funcions que duu a terme la signatura electrònica són:

- Autenticació d'una persona o entitat prèviament identificada.
- Autenticació de l'origen d'unes dades.
- Declaració de coneixement.
- Declaració de voluntat.

Algunes de les tecnologies que permeten complir determinades, o bé totes, aquestes funcions són:

- Signatura amb llapis digital al realitzar pagaments amb targeta de crèdit.
- Marcant la casella d'acceptació de termes i condicions en pàgines web.
- Utilitzant l'usuari i contrasenya.
- Utilitzant l'anomenada **signatura digital**.

2.4.2 Signatura digital

De tots els tipus de signatura electrònica que acabem de veure, el que ens interessa a nivell criptogràfic és el de **signatura digital**. Aquest concepte va ser introduït a l'any 1976 pels criptògrafs estatunidencs **Bailey Whitfield "Whit" Diffie** (5 de Juny de 1944) i **Martin Edward Hellman** (2 d'Octubre del 1945) (creadors de l'algoritme de Diffie-Hellman per a l'intercanvi de claus, comentat anteriorment).

La signatura digital és un mètode criptogràfic que associa la identitat d'una persona o entitat, o d'un equip informàtic concret, al missatge o document que es vol enviar. Es compleixen tres propietats importants:

- **Integritat**: la signatura digital assegura la integritat del missatge enviat. El receptor pot verificar que les dades rebudes no han estat modificades durant la seva transmissió.
- **Autenticació**: el receptor pot determinar la persona o entitat creadora del missatge rebut.
- **No repudi**: l'emissor no pot negar l'autenticitat de la seva signatura.

Per tant, un sistema segur de signatura digital constarà de dues parts: per una banda un mètode per signar els documents, de tal manera que sigui impossible la falsificació, i per un altre, un mètode per tal de verificar que la firma va ser generada per la persona que diu haver-la generat.

No s'ha de confondre el concepte de "signatura electrònica" i el de "signatura digital". Podem dir que "signatura electrònica" és un concepte més ampli, i estableix un marc jurídic que li dóna validesa legal. La signatura digital, es refereix únicament als mètodes criptogràfics que permeten la seva creació.

Per a realitzar una signatura digital d'un document, la primera cosa que s'ha de fer, és aplicar-li un algoritme matemàtic anomenat **funció de HASH**. Aquest algoritme permet calcular un valor resum de les dades que seran firmades digitalment. Al resum resultant del text inicial, s'aplica l'**algoritme de signatura**, generant llavors l'anomenada signatura digital. Els algoritmes per generar la signatura digital poden ser de clau privada o de clau pública. Entre els de clau privada, destaquen algoritmes com:

- Signatura de Lamport-Diffie.
- Signatura de clau simètrica de Rabin.
- Signatura de Desment.

Però són més coneguts i emprats els algoritmes de signatura digital de clau pública, tals com:

- Signatura RSA.
- Signatura DSS.
- Signatura ElGamal.
- Signatura de corbes el·líptiques.
- Signatura de ESING.
- Signatura de clau asimètrica de Rabin.

En certes ocasions la signatura digital porta implícit l'anomenat **Timestamp**, o Segell de Temps. Aquest segell és una marca temporal que estableix en quin moment concret ha estat generada la

signatura, i per tant, es pot utilitzar per establir uns períodes durant els quals aquesta signatura és vàlida.

Les aplicacions de la signatura digital són molt diverses. Es poden fer servir per:

- Factures electròniques.
- Contractes comercials electrònics.
- Transaccions comercials electròniques.
- Vot electrònic.
- Notificacions judicials electròniques.

Són moltes altres les aplicacions de la signatura digital, però ens hem limitat en aquest apartat a donar una breu pinzellada sobre el seu funcionament i aplicacions. Seguidament, farem un anàlisi més detallat sobre el seu funcionament a nivell criptogràfic.

2.4.3 Funció de HASH

Podem definir un **HASH** com a un **número resum**. Si disposem d'un document qualsevol, un algoritme de HASH és una funció que, a partir de la sèrie de bits que formen aquest document, ens dóna com a sortida un altre conjunt de bits que resumeixen el seu contingut, i que depenen, bit a bit, del flux d'entrada. El valor resum o HASH, és de longitud fixa, i aquesta longitud depèn de l'algoritme emprat per al seu càlcul. És a dir, tots els HASH generats amb un algoritme determinat tindran la mateixa longitud independentment de l'entrada de l'algoritme.

El càlcul del HASH de qualsevol document, s'ha de poder realitzar de forma fàcil i ràpida mitjançant equipament informàtic. El funcionament dels algoritmes de HASH és d'**una única direcció**, és a dir, es pot calcular el valor resum d'un text determinat, però no es pot, a partir del resum, obtenir de nou el document inicial. El resultat de la funció és un número que identifica, inequívocament al text original. No ha d'ésser possible construir un document que generi, amb l'aplicació de l'algoritme, un HASH determinat.

L'algoritme de HASH no és, en sí mateix, un algoritme d'encriptació, però si que s'utilitzen en esquemes de xifrat, com algoritmes de xifrat asimètric del tipus RSA. Les **funcions** per les que s'empra un algoritme de HASH poden ser variades, com per exemple:

- **Comprovació de la integritat** dels fitxers. Si abans d'enviar un determinat document, s'aplica una funció de HASH, i s'envia juntament amb el fitxer original el HASH resultant, és factible per al receptor tornar a fer el càlcul del HASH del document rebut, i comparar-lo amb l'enviat per part de l'emissor. Si els dos coincideixen, es pot assegurar la integritat del document enviat. Aquesta és una funció molt estesa, per exemple, per la comprovació de la integritat dels paquets d'actualització dels sistemes GNU/Linux.
- **Seguretat als processos d'autenticació d'usuaris**. L'algoritme de HASH afegeix més seguretat als entorns d'autenticació d'usuaris mitjançant login i password. Si l'emmagatzemament d'aquestes dades no es realitza com a text clar, si no que s'emmagatzemen les dades resultant d'aplicar un algoritme de HASH, el fet que un usuari maliciós obtingués accés a les dades emmagatzemades no comprometria la seguretat del sistema, donat que no podria obtenir el login i password originals a partir del resultat de la funció de HASH. Això serveix tant en entorns de sistemes operatius com en entorns web.
- El cas que més ens interessa, per a la signatura digital. Els algoritmes de HASH serveixen per a verificar la **integritat** de la informació enviada. A més, en determinats procediments criptogràfics, no es xifrarà el missatge complet, sinó el resultat de la funció de HASH del missatge original (és molt útil en procediments de clau pública, donat que els requeriments computacionals per al xifrat són elevats, i és més eficient aplicar l'algoritme d'encriptació a un HASH que al missatge complet).

Entre els algoritmes de HASH més importants trobem el MD-5 i el SHA-1. Seguidament en farem un anàlisi més detallat.

2.4.3.1 MD-5

El MD-5 (Message Digest-5) és un dels algoritmes de reducció creats per Ronald Rivest, professor del MIT(Massachusetts Institute of Technology). Va ser dissenyat al 1991, en substitució del seu predecessor, el MD-4, quan Hans Dobbertin va descrobrir-ne una debilitat. El MD-5

processa missatges de mida arbitrària, en blocs de 512 bits, i generant una sortida de 128 bits. Amb la capacitat de processament dels equips informàtics actuals, aquesta mida s'ha demostrat insuficient. A més, de diversos atacs criptoanalítics, la demostració al 1996 d'una col·lisió de HASH (situació en la qual, dos missatges d'entrada diferents generen el mateix HASH a la sortida) per part de Hans Dobbertin, han fet que el MD-5, tot i ser un dels algoritmes més estesos, comenci a plantejar dubtes sobre el seu futur, i diversos investigadors recomanin substituir-lo per altres algoritmes alternatius com el SHA-1.

2.4.3.2 SHA-1

El SHA-1 (Secure Hash Algorithm 1) és un sistema de funcions de HASH criptogràfiques de la NSA (National Security Agency) dels Estats Units, i publicades pel NIST(National Institute of Standards and Technology). Va sorgir com a successor del SHA (conegut actualment i de forma oficiosa com a SHA-0, per evitar malentesos). El SHA-1 pot realitzar resums HASH de missatges d'una longitud màxima de 2^{64} bits. Això equival a més de dos mil milions de gigabytes. El HASH resultant té una mida de 160 bits (per 128 de l'algoritme SHA original). Noves i més avançades versions del SHA modifiquen certes parts del disseny, i produeixen sortides amb mides que van des dels 224 fins als 512 bits, rebent tots ells el nom genèric de SHA-2.

Va ser a l'any 2004 quan un grup d'investigadors xinesos, Xiaoyun Wang, Yiqun Lisa Yin i Hongbo Yu (de la *Shandong University* a Xina) van trobar debilitats al MD-5, tals que comprometen la seguretat d'aquest algoritme. Tenint en compte que SHA-1 té una estructura similar, i es basa en principis matemàtics similars als emprats per Ronald Rivest al MD-5, es comencen a plantejar dubtes sobre la seguretat que pot aportar també el SHA-1 en el futur. El grup d'investigació xinès va demostrar la possibilitat de trencar el SHA-1 en 2^{69} operacions, i posteriorment s'ha reduït inclús més, fins a 2^{63} . Segons el NIST, aquest és encara un nombre elevat d'operacions, però entra ja dintre de les capacitats computacionals actuals, de la qual cosa es dedueix que, en relativament poc temps, trencar el SHA-1 estarà a l'abast de molts computadors, amb la millora de les capacitats de procés dels equips, i amb el refinament dels atacs criptogràfics. Els atacs per col·lisió de HASH suposen un problema menys important, donat que trobar dos missatges que generin el mateix HASH, i que els dos siguin congruents, i a més tinguin sentit amb el context de la conversació és gairebé impossible. Tot i que el NIST contempla els SHA-2 amb sortida de major mida de bits, són molts els experts que proposen la cerca d'una nova funció de HASH que serveixi com a estàndard, i que substitueixi al SHA-1. Alguns dels candidats són l'algoritme TIGER, dels creadors de SERPENT, i WHIRLPOOL, dels creadors del AES.

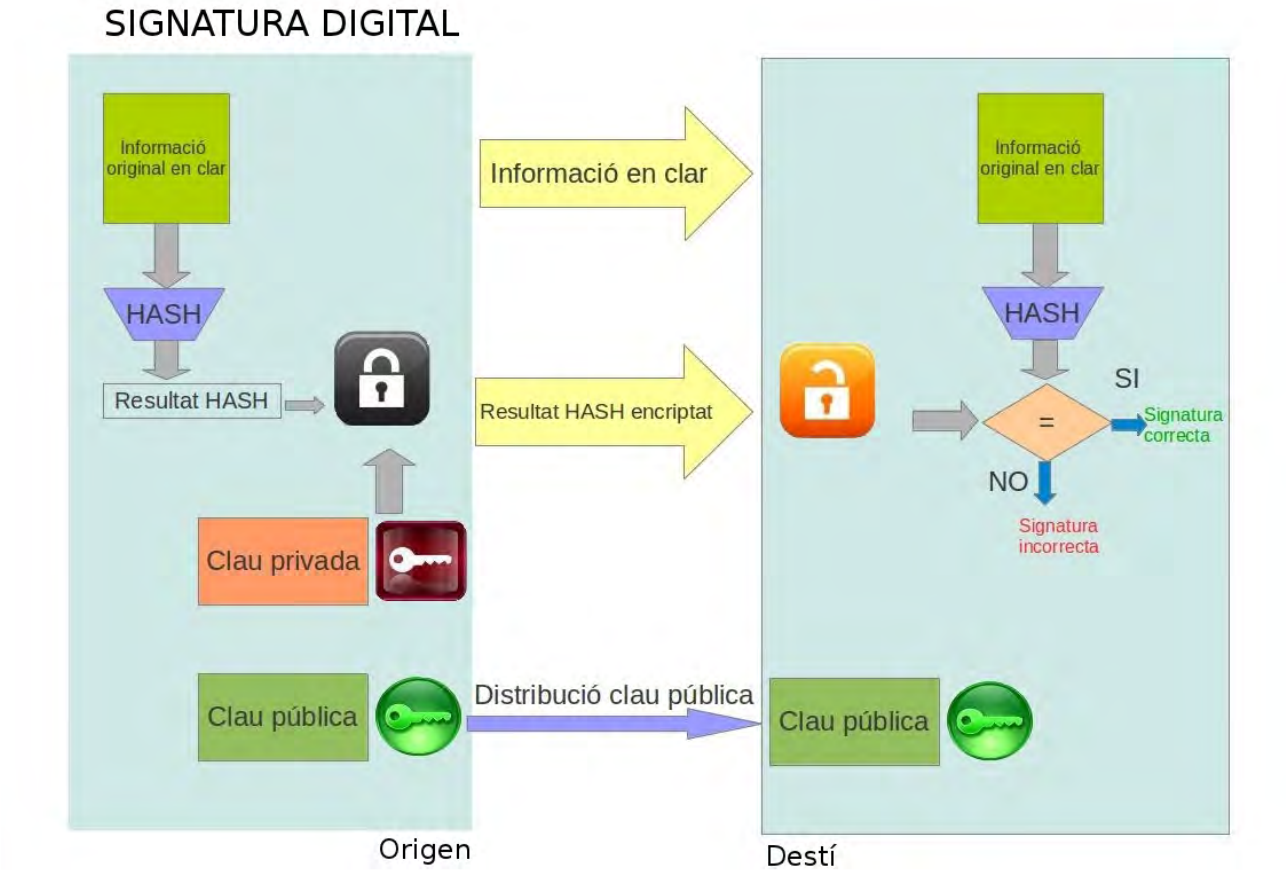
2.4.4 Resum-Conclusions

La signatura digital es fa necessària en entorns en els que es vol obtenir fiabilitat sobre l'emissió de les dades. Donat que la major part de les comunicacions es realitzen sobre el protocol TCP/IP, i aquest no va ser dissenyat per a oferir comunicacions segures sobre Internet, qualsevol usuari maliciós podria interceptar missatges de la xarxa i modificar-los, o directament enviar missatges suplantant la identitat d'algú altre. Per evitar aquests problemes, s'ha fet necessària la implantació del sistema de signatura digital.

La signatura digital és, doncs, un equivalent a la signatura física o escrita, dissenyada per que pugui ser aplicada en entorns de transmissió digital. Per tant, és un mètode mitjançant el qual el destinatari d'un determinat missatge o document pot verificar que les dades rebudes no han estat alterades durant la transmissió i que l'emissor és efectivament la persona que diu ser. A més, l'emissor no pot negar ser ell qui ha signat el document o missatge.

La signatura digital té la mateixa validesa que la signatura física, i per aquest motiu diverses administracions públiques ja utilitzen aquest tipus de tecnologia per a la identificació dels usuaris de les aplicacions destinades als serveis al ciutadà.

El funcionament de la signatura digital en un entorn de comunicació amb procediment de clau pública queda resumit en el següent esquema (Il·lustració 21):



Il·lustració 21: Diagrama del procés de signatura digital

L'emissor vol transmetre un missatge o document a un determinat destinatari. Per tal d'assegurar

que les dades que arribaran a l'altre extrem de la comunicació són les correctes, utilitzarà la seva signatura digital. En primer lloc, la informació del missatge o document en clar serà utilitzada com a entrada de l'algoritme de HASH o resum. El resultat de l'aplicació d'aquest algoritme de HASH tindrà un format concret amb una longitud fixa.

En criptosistemes de clau pública, per assegurar una bona robustesa de l'algoritme emprat, la mida de la clau ha de ser relativament llarga. Per aquest motiu, l'aplicació de l'algoritme d'encriptació no es realitza sobre les dades originals, que podrien ser d'una mida considerable, i endarrerir l'execució més del desitjable. Es realitza sobre el resultat de la funció de HASH que prèviament s'ha aplicat a aquestes dades. La clau que s'ha de fer servir per a aquesta encriptació és la clau secreta, aquella que només coneix l'emissor, i que ha d'estar sota el seu control exclusiu i no ha de ser coneguda per cap altra persona. Les dades resultants d'aplicar l'algoritme d'encriptació al HASH o resum del document original seran la signatura digital d'aquest document.

Realitzats aquests passos, l'emissor enviarà les dades originals al receptor, i juntament amb aquestes, enviarà la signatura digital que s'ha generat. Amb aquests dos elements, l'usuari receptor pot comprovar, gràcies a la clau pública de l'emissor, que les dades són correctes.

Per tal de comprovar la integritat del missatge, el receptor aplica l'algoritme de desxifrat del criptosistema corresponent, utilitzant la clau pública de l'emissor, i que ha de ser de domini públic. El que obtindrà serà el resultat de la funció de HASH que ha aplicat prèviament l'emissor, i que ha transmès juntament amb les dades originals. El receptor aplica el mateix algoritme de HASH al missatge original en clar que li ha enviat l'emissor. Si el resultat d'aquest algoritme de HASH no és el mateix que el que ha obtingut després de desxifrar mitjançant la clau pública, el receptor pot deduir que les dades han estat alterades durant la transmissió, ja sigui de forma malintencionada, o bé per problemes al mitjà de transmissió. En aquest cas, la signatura digital es considera incorrecta, donat que no es pot donar validesa a la integritat de les dades rebudes, i no es pot assegurar que l'autor sigui la persona que ens ha enviat les dades. El suposat emissor pot, doncs, repudiar l'autoria del document enviat.

Si, en canvi, el receptor aplica l'algoritme de desxifrat a les dades rebudes, i el resultat obtingut és el mateix que el que ell calcula aplicant la mateixa funció de HASH a les dades originals que també li han estat transmeses, el receptor pot estar segur de la integritat de les dades que ha rebut, i de l'autoria del missatge per part de l'emissor. L'emissor tampoc pot negar ser l'autor de les dades rebudes a l'altre extrem de la comunicació. La signatura és en aquest cas vàlida.

3 DNI-Electrònic

3.1 Introducció

En els darrers anys, les comunicacions telemàtiques han experimentat uns grans canvis, deguts principalment a l'aparició i generalització de l'ús d'Internet. Són molts els efectes positius derivats de la possibilitat de comunicar-se a grans distàncies amb altres persones o entitats de forma ràpida i assequible. Però s'ha fet necessària l'aparició de mitjans que donin seguretat i validesa a aquestes comunicacions, generant confiança entre les persones per a l'ús de les noves tecnologies per a les comunicacions.

En resposta a aquestes necessitats, l'Administració Pública espanyola va aprovar l'entrada en vigor del nou DNI-Electrònic, començant a emetre'l des del Març de 2006. El DNI-Electrònic és la evolució del DNI tradicional, adaptant-lo a la societat de la informació en la qual vivim, i permetent als seus usuaris comunicacions segures i vàlides a través dels canals telemàtics existents.

Amb el DNIe s'aconsegueix atorgar als ciutadans la capacitat d'acreditar la seva identitat als participants en una comunicació digital, i assegurar la procedència i la integritat dels missatges intercanviats. Per tal d'aconseguir-ho, el DNIe conté:

- Uns certificats de ciutadà **X509v3**(donarem una explicació més acurada més endavant):
  - Un per a la **autenticació d'identitat**: El ciutadà podrà, a través d'aquest certificat, autenticar la seva identitat davant de tercers, demostrant la possessió i l'accés a la clau privada associada a aquest certificat, i que acredita la seva identitat.
  - Un per a la **signatura**, que permetrà realitzar accions i assumir compromisos electrònicament, podent ser comprovada la integritat dels documents signats mitjançant els instruments de signatura inclosos en ell.
- Unes **claus privades** associades que es generen i insereixen durant el procés d'expedició.

És destacable la existència al DNIe de dos certificats diferents, un d'autenticació d'identitat, i un altre per a la signatura electrònica. És així en un intent per fer que el ciutadà distingeixi entre els dos procediments independentment de la similitud dels processos criptogràfics.

Entre les diferents funcions que es poden realitzar amb seguretat amb el DNIe, trobem:

- Realitzar compres signades a través d'Internet.
- Realitzar tràmits complets amb les Administracions Públiques a qualsevol hora, sense la necessitat de realitzar desplaçaments, i sense temps d'espera ni cues.
- Realització de transaccions segures amb entitats bancàries.
- Accés a l'edifici on el ciutadà té el seu lloc de treball.
- Utilitzar el nostre ordinador de forma segura, gràcies a la validació amb DNIe.
- Participar en converses a través d'Internet, amb la seguretat que el nostre interlocutor és qui diu ser.

3.2 Requisits

Per a poder emprar el DNIe i els certificats continguts en ell, és necessari que l'usuari disposi d'una sèrie d'elements hardware i software compatibles.

El maquinari necessari és:

- Un ordinador personal (Intel, amb processador Intel Pentium III o superior, o tecnologia equiparable).
- Un lector de targetes intel·ligents, o Smart Card. S'ha de verificar que compleixi, almenys, aquests requeriments:
  - Ha de complir l'estàndard ISO-7816 (1, 2 i 3).
  - Ha de suportar targetes asíncrones basades en protocols T=0 (i T=1).
  - Ha de suportar velocitats de, com a mínim, 9600bps.
  - Ha de suportar els estàndards:
    - API PC/SC (Personal Computer/Smart Card).
    - CSP (Cryptographic Service Provider, Microsoft).
    - API PKCS#11.

El programari necessari és:

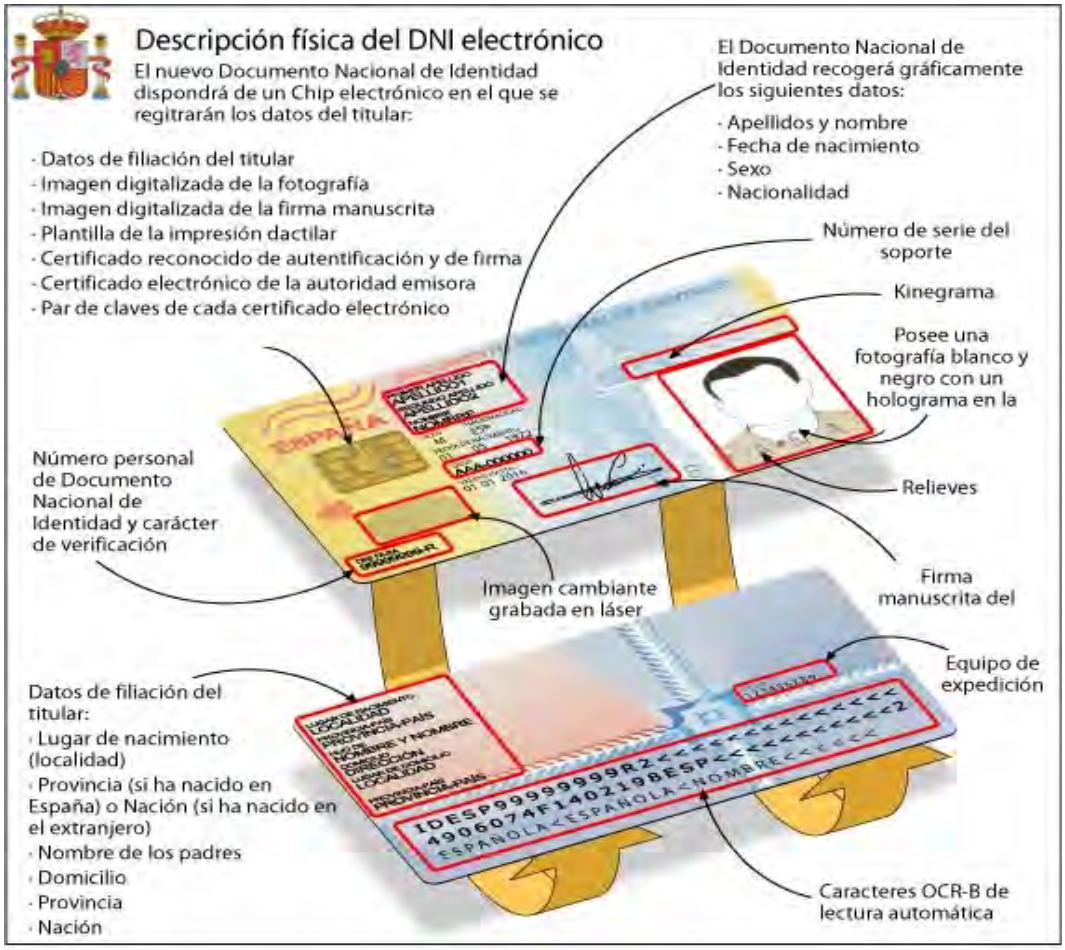
- Sistemes operatius:
  - Microsoft Windows (XP, Vista, 7 i 8).
  - Linux (la majoria de distribucions).
  - Unix.
- Navegadors:
  - Microsoft Internet Explorer (versió 6.0 o superior).
  - Chrome.
  - Mozilla Firefox (versió 1.5 o superior).
  - Netscape (versió 4.78 o superior).
- Controladors de la lectora Smart Card, i que seran específics en funció del fabricant i model de la lectora, i del sistema operatiu en el qual s'estan executant.
- Mòduls criptogràfics. Aquests poden ser descarregats des de la web http://dnielectronico.es/descargas
  - En entorns **Microsoft Windows**, l'equip ha de tenir instal·lat un servei denominat **Cryptographic Service Provider** (CSP) amb navegadors **Mozilla Firefox**, o el **Smart Card Mini-Driver** amb navegadors **Internet Explorer** o **Chrome**.
  - En entorns **Unix/Linux** o **Mac**, el DNIe es pot emprar a través del mòdul criptogràfic **PKCS#11**.

3.3 Característiques

El **DNIe** (Il·lustració 22), expedit per la Direcció General de la Policia, ha estat **dissenyat per a complir els estàndards**, tant a nivell físic com critptogràfic, que estipula la Unió Europea en quant a documents d'identificació personal. A nivell físic:

- La targeta física del DNIe segueix l'estàndard ISO-7816-1.
- Fabricada en policarbonat, un material altament resistent per al seu ús durant el període de vigència del DNI, és a dir, 10 anys.
- Les dades de filiació, la fotografia i la signatura manuscrita són gravades al cos de la targeta mitjançant tecnologia làser, garantint d'aquesta forma la impossibilitat de la manipulació d'aquestes dades.
- Està dotat de moltes i molt modernes mesures de seguretat, que es poden dividir en tres nivells. En primer lloc trobem els hologrames, les lletres tàctils, les imatges tàctils, les imatges làser canviants i les tintes especials entre altres. El segon nivell són les imatges codificades, els microtexts i els kinegrames (tecnologia desenvolupada per l'empresa suïssa Kinegram que conté uns tipus especials d'elements òptics difractius generats per ordinador amb relleus simètrics i asimètrics a la seva superfície). Per últim, hi trobem mesures de seguretat criptogràfiques i biomètriques. Totes aquestes mesures fan del DNIe un document altament segur tant a nivell físic com electrònic.

Passarem seguidament a realitzar un repàs de les dades contingudes al DNIe:



Il·lustració 22: Descripció del DNIe

En l'anvers:

- Al cos central del document trobem:
  - Primer cognom del ciutadà.
  - Segon cognom del ciutadà.
  - Nom del ciutadà.
  - Sexe i nacionalitat del ciutadà.
  - Data de naixement del ciutadà.
  - El IDESP, número de sèrie del suport físic de la targeta.
  - Data de validesa del document.
- A la part inferior esquerra:
  - Número del Document Nacional d'Identitat del ciutadà, seguit del caràcter de verificació. Conjuntament formen l'anomenat NIF, Número d'Identificació Fiscal.
- A l'espai destinat a la impressió de la imatge làser canviant:

- La data d'expedició del document en format DDMMAA.
- La primera consonant del primer cognom més la primera consonant del segon cognom més la primera consonant del nom (del primer nom en cas de ser un nom compost).

- Xip criptogràfic que conté diversa informació en format digital.
  - Un certificat electrònic per autenticar la identitat del ciutadà.
  - Un certificat electrònic per signar digitalment, amb la mateixa validesa jurídica que la signatura manuscrita.
  - Certificat de la Autoritat de certificació emissora.
  - Claus per al seu ús.
  - La plantilla biomètrica de la impressió dactilar del ciutadà.
  - La fotografia digitalitzada del ciutadà.
  - La imatge digitalitzada de la signatura manuscrita del ciutadà.
  - Les dades de la filiació del ciutadà, corresponents amb el contingut personalitzat de la targeta.
- Elements de seguretat del document per evitar la seva falsificació:
  - Mesures físiques:
    - Visibles a simple vista com les tintes òpticament variables, relleus i els fons de seguretat.
    - Verificables gràcies a mitjans òptics i electrònics, com són les tintes visibles únicament amb llum ultraviolades, o la microescriptura.
  - Mesures digitals:
    - Encriptació de les dades del xip.
    - Accés a la funcionalitat del DNIe mitjançant la clau personal d'accés (PIN).
    - Les claus que mai abandonen el xip.
    - La Autoritat de Certificació és el de la Direcció General de Policia.
- Al revers trobarem:
  - Informació impresa visible a simple vista:
    - Lloc de naixement.
    - Província-País.
    - Nom dels pares.
    - Domicili.
    - Lloc de domicili.
    - Província-País i Equip.
  - Informació impresa OCR-B per a lectura mecanitzada sobre la identitat del ciutadà

segons la normativa OACI per a documents de viatge.

L'element més destacable del nou DNIe és el microxip que porta incorporat. Les seves característiques són:

- **Xip ST19WL34**.
- **Sistema operatiu DNIe v1.1**.
- **Capacitat de 32KB**.

El contingut del xip està distribuït en tres zones amb diferents nivells i condicions d'accés:

- Zona pública accessible en lectura i sense restriccions:
  - **Certificat de la CA** intermitja emissora.
  - **Claus Diffie-Hellman**.
  - **Certificat X509 de component**: el seu propòsit és l'autenticació de la targeta del DNIe mitjançant el protocol d'autenticació mútua definit en CWA 14890.
    - Permet l'establiment d'un canal xifrat i autenticat entre la targeta i els drivers.
    - No estarà accessible directament per les interfícies estàndard (PKCS11 o CSP).
- Zona privada accessible per a lectura pel ciutadà mitjançant l'ús de la clau personal d'accés PIN:
  - **Certificat de signatura**: garanteix la integritat i el no repudi del document enviat. És un certificat X509v3 estàndard, que té actiu en el Key Usage el bit de Commitment(no repudi) i està associat a un parell de claus pública i privada, generades a dins del xip del DNIe.

    És aquest certificat expedit com a certificat reconegut i creat en un Dispositiu Segur de creació de signatura, el que converteix la signatura electrònica avançada en signatura electrònica reconeguda, permetent la equiparació amb la signatura manuscrita.
  - **Certificat d'autenticació** (Digital signature): aquest certificat garanteix la identitat del ciutadà a les transaccions telemàtiques. El certificat d'autenticació assegura que el titular és qui diu ser, i li permet acreditar la seva identitat en front d'altres, ja que posseeix el certificat d'identitat, i la clau associada al mateix.

    Aquest certificat no és hàbil en operacions que requereixin no repudi d'origen, per la qual cosa els receptors no tindran garantia de compromís del titular del DNIe amb el contingut signat. El seu ús serà més aviat per a l'accés segur a sistemes informàtics(establint canals segurs i confidencials amb els prestadors de serveis).

    Es pot utilitzar també com a mitjà d'identificació per a la realització d'un registre que permeti la expedició de certificats reconeguts per part d'entitats privades sense l'obligació de fer una gran inversió en la creació i manteniment d'una infraestructura de registre.

- Zona de seguretat accessible per a lectura pel ciutadà als punts d'actualització del DNIe.

- **Dades de filiació del ciutadà** (els mateixos que estan físicament escrits a la targeta).
- Imatge de la **fotografia**.
- Imatge de la **signatura manuscrita**.

Les dades criptogràfiques que conté són:

- **Clau RSA pública d'autenticació** (Digital Signature).
- **Clau RSA pública de no repudi** (CommentCommitment).
- **Clau RSA privada d'autenticació** (DigitalSignature).
- Clau RSA de signatura(ContentCommitment).
- Patró d'impressió dactilar.
- Clau Pública de root CA per certificats card-verificables.
- Claus de Diffie-Hellman.

Dades de Gestió:

- Traça de fabricació.
- Número de sèrie del suport.

- Zona lògica inaccessible. Només accessibles a través del microxip, aquesta zona es refereix a les claus privades RSA, i al model d'impressió dactilar.

3.4 Seguretat

El DNIe conté un sèrie de mesures de seguretat.

- Autenticació: La targeta del DNIe disposa de diferents mètodes, mitjançant els quals una entitat externa demostra la seva identitat, o el coneixement d'alguna dada secreta emmagatzemada en la pròpia targeta. Si aquests mètodes es realitzen de forma correcta, ens permet obtenir unes condicions de seguretat que podran ser requerides per a l'accés a diversos recursos del DNIe.

  - Autenticació mitjançant el Número d'Identificació Personal (PIN).

    La targeta del DNIe està dissenyada per suportar la verificació d'usuari (CHV-Card Holder Verification). Aquesta operació es realitza comprovant el codi facilitat per la entitat externa a través de la corresponent comanda. Cada codi CHV conté un comptador d'intents. Aquest comptador es va decreixent en una unitat per cada intent incorrecte d'introducció del PIN. Tornarà a l'estat inicial després d'una presentació correcta del PIN. Habitualment el nombre d'intents erronis serà 3. Si aquest comptador arriba a zero, la targeta quedarà bloquejada. Per desbloquejar-la cal realitzar una presentació de l'empremta dactilar als centres de DNIe habilitats a tal efecte. També existeix un nombre màxim d'intents de presentació de l'empremta dactilar. Si s'esgoten els intents, no és possible el desbloqueig de la targeta.

    És important dir que el PIN es pot modificar presentant el seu valor actual, o bé

l'empremta dactilar. El PIN és personal i intransferible, únicament conegut pel titular del DNI-e.

- Autenticació mitjançant dades biomètriques.

  El DNIe permet la identificació del titular a través de mètodes biomètrics, però aquesta funció només estarà disponible a punts d'accés controlats.

  L'aplicació decidirà, un cop coneguda la informació sobre les empremtes emmagatzemades a la targeta, quina d'elles passarà a verificar, sol·licitant la col·locació del dit corresponent a l'equipament dissenyat a tal efecte. Un cop obtinguda l'empremta, es presenta la informació biomètrica a la targeta, i aquesta, mitjançant un algoritme Match on Card, avalua la correspondència amb la empremta emmagatzemada. Si aquesta correspondència és correcta, es pot donar la verificació com a vàlida. Si no és així, restarà un als intents de presentació de l'empremta dactilar.

- Autenticació d'aplicació.

  Aquest mètode d'autenticació té com a finalitat que una entitat externa demostri tenir coneixement del nom i valor d'un codi secret. Per a fer-ho, es fa servir un protocol de desafiament-resposta, mitjançant aquests passos:

  - L'aplicació demana un desafiament a la targeta.
  - L'aplicació ha d'aplicar un algoritme a aquest desafiament juntament amb el corresponent codi secret i nom de la clau.
  - La targeta realitza la mateixa operació i compara el resultat amb les dades transmeses per l'aplicació. Si coincideixen, es considera correcte per a la realització d'operacions posteriors.

- Autenticació mútua.

  Aquest mètode permet que ambdues parts de la conversa (targeta i aplicació externa) puguin confiar en l'altra gràcies a la presentació de certificats i la seva validació.

  El procés s'inicia amb l'intercanvi segur de claus de sessió. Aquestes claus seran utilitzades posteriorment per a encriptar la resta de missatges. Es poden seleccionar diferents alternatives, tant de forma implícita com explícita. Aquestes alternatives estan basades en la especificació 'CWA 14890-1 Application Interface for Smart Cards used as Secured Signature Creation Devices – Part 1', i són:

  - Autenticació amb intercanvi de claus.
  - Autenticació de dispositius amb protecció de la privacitat.

- Securització de missatges.

  Per a la comunicació "un a un", el DNIe dóna la possibilitat d'establir un canal segur entre les dues parts de la conversa mitjançant l'autenticació del terminal i targeta gràcies a l'ús dels certificats. Un cop establert aquest canal segur, els missatges enviats per ambdues parts es xifren i autentiquen, assegurant la comunicació als dos punts de la comunicació. Aquest canal segur pot ser requerit per l'aplicació, o bé pot ser una restricció d'accés a algun dels recursos integrats a la targeta del DNI-e.

  Per establir el canal segur, es realitza primerament l'intercanvi de claus públiques entre targeta i terminal, mitjançant la verificació dels certificats. Amb un protocol d'autenticació

mútua, en el que cada part envia una clau a l'altra, derivant juntes a una clau comuna, es generen les claus de sessió per al xifrat i l'autenticació. Un cop es tenen les claus, tots els missatges s'hauran d'enviar securitzats.

- Desbloqueig i canvi del PIN.

  És possible el canvi del valor del PIN de dues formes: o bé presentant el valor antic, o bé mitjançant l'ús de les dades biomètriques, és a dir, l'empremta dactilar a determinades instal·lacions destinades a tal efecte.

  Donat que el canvi de PIN és un punt crític per a la seguretat del funcionament del DNI-e, aquest canvi només pot realitzar-se sota determinades condicions. És necessària la màxima confidencialitat i l'establiment d'un canal segur. Per això és exigible l'existència de determinades condicions de seguretat, o bé realitzar el canvi als terminals instal·lats a les dependències del centres habilitats per a l'expedició del DNI-e. El canvi del PIN mitjançant la presentació de l'empremta dactilar està permès únicament en aquests terminals.

- Funcionalitat criptogràfica.

  La targeta del DNIe té la capacitat de **generar i gestionar claus RSA**. La generació del parell de claus RSA segueix l'algoritme estàndard PKCS#1 v1.5. S'empra l'algoritme Miller Rabin com a test de primalitat.

  El DNIe també és capaç de fer **HASH** de dades mitjançant l'**algoritme SHA1**. Tot el procés es pot realitzar en la pròpia targeta, o finalitzar un HASH calculat de forma externa. En qualsevol cas, al finalitzar una operació de HASH, el codi resultant és emmagatzemat a la memòria del DNIe per a poder ser utilitzat posteriorment. El HASH romandrà a memòria fins a la següent operació.

  Entre les capacitats criptogràfiques disponibles, també trobem la de la signatura electrònica en dos modes diferents: Mode **raw**, i mode **emplenament PKCS#1**.

- Intercanvi de claus.

  L'operació d'intercanvi de claus és emprada per compartir claus simètriques o de sessió entre dues entitats. És possible xifrar una clau Ks utilitzant la clau pública d'un destinatari, la qual pot ser carregada a la memòria de la targeta i protegida mitjançant una clau RSA. El destinatari pot desxifrar la clau Ks emprant la seva clau privada RSA corresponent.

- Xifrat

  Amb el DNIe es poden realitzar xifrats 3DES CBC amb claus de 16 bytes (k1, k2, k1). Per a realitzar aquestes operacions la clau de 16 bytes ha de ser emmagatzemada en la memòria de l'equip. Aquest algoritme està protegit per l'algoritme RSA. La clau de 16 bytes romandrà en memòria fins que finalitzi la sessió, o es carregui una de nova.

3.5 Utilització

Com s'ha comentat amb anterioritat, per a l'ús del DNIe és necessari disposar, a més del propi DNI amb capacitats electròniques, d'un equip informàtic amb un lector de Smart Card compatible PC/SC i del mòdul criptogràfic adient per al sistema operatiu i navegador en el qual s'està treballant. En connectar-se a un servei telemàtic d'una Administració Pública o entitat privada a través d'Internet, s'estableix un canal privat i autenticat per les dues parts entre el ciutadà i la entitat. Normalment, aquest canal segur es correspondrà a una sessió SSL (Secure Socket Layer), ja que gairebé el 100% dels servidors i clients emprats disposen d'aquesta capacitat. Existeixen dos tipus de canals SSL:

- **Autenticació Servidor**: només el servidor necessita tenir un certificat. Així, la identitat del client, en aquest cas el ciutadà, serà anònima.
- **Autenticació Servidor-Client**: requereix que servidor i client, és a dir, Administració i ciutadà s'autentifiquin enfront de l'altre. Aquest és l'ideal i recomanat. La diferència radica en que, al tenir l'Administració Pública garantia de la identitat del ciutadà, li pot oferir serveis i informació específics per a ell.

Les parts implicades en l'establiment d'un canal segur són:

- El **DNIe** en possessió del ciutadà, i emès per la Direcció General de Policia.
- El propi **ciutadà**, és a dir, el titular del DNI-e.
- L'**Administració Pública o entitat privada** que proveeix un servei.
- Una **Autoritat de Validació** que informa de la validesa o no dels certificats del ciutadà.

L'**esquema** per a l'establiment de la sessió **SSL** amb autenticació **Servidor-Client** serà el següent:

1) Petició per part del ciutadà d'una connexió segura i autenticada.
2) L'Administració Pública o entitat privada crea un missatge autenticat i l'envia al ciutadà.
3) El ciutadà verifica la validesa del certificat de servidor rebut.
4) Es genera la clau de sessió i xifrat de la mateixa amb la clau pública de l'Administració Pública o entitat privada.
5) Es genera el missatge d'intercanvi de claus.
6) Amb el DNIe introduït al lector, i mitjançant el certificat d'autenticació, el ciutadà valida el missatge d'intercanvi de claus.
7) S'estableix un canal privat.
8) L'Administració Pública o entitat privada verifica el missatge d'establiment de sessió.
9) L'Administració Pública o entitat privada comprova a l'Autoritat de Validació l'estat del Certificat d'Autenticació del Ciutadà.
10) S'estableix un canal segur i es tanca el túnel SSL.

Com es pot comprovar en aquest esquema, per a dur a terme el procés d'autenticació entre les dues parts de la comunicació per a l'establiment d'un canal segur, es fa servir:

- El **certificat de l'Administració Pública o entitat privada**. Aquest certificat està associat al servidor de l'Entitat pública o privada amb la qual s'estableix la comunicació, garantint que la connexió es realitza amb aquesta entitat i no una altra. Aquest certificat no l'emet la Direcció General de la Policia ni el Ministeri d'Interior, si no que ha de ser garantit per una **Autoritat de Certificació** diferent de la DGP, subjecta a la Llei 59/2003 en el marc de les obligacions aplicables als prestadors de serveis de certificació.
- **Certificat d'autenticació del ciutadà**. Per poder-se identificar davant d'una Administració Pública o entitat privada, el ciutadà disposa d'un certificat a tal efecte. L'Administració Pública o entitat privada pot determinar la identitat del ciutadà i oferir un servei personalitzat. La veracitat d'aquest certificat si que ve determinada per la Direcció General de Policia.

En quant a la signatura de tràmits administratius amb el DNI-e, el següent esquema estableix el protocol a seguir per a la signatura de formularis electrònics, complint amb la normativa subjecta als certificats qualificats:

1) L'Administració Pública o entitat privada envia el formulari per al tràmit administratiu.
2) El ciutadà omple les dades del formulari i l'envia.
3) L' Administració Pública o entitat privada reconstrueix el formulari en format text i l'envia de nou al ciutadà.
4) El ciutadà verifica que el tràmit en format text es correspon a les dades introduïdes.
5) Se li sol·licita al ciutadà la signatura electrònica del formulari.
6) El ciutadà introdueix el seu número d'identificació personal (PIN) per accedir al certificat de signatura.
7) El DNIe signa el formulari.
8) El ciutadà envia a l' Administració Pública o entitat privada el formulari signat.
9) L' Administració Pública o entitat privada comprova la validesa de la signatura, i la integritat de les dades.
10) L' Administració Pública o entitat privada comprova la validesa del certificat de signatura del DNIe amb la Autoritat de Certificació.
11) Si tots aquests passos són correctes, es pot continuar amb el procediment.

Per a dur a terme el procés de signatura electrònica, s'ha de disposar d'una aplicació informàtica que permeti realitzar aquesta funcionalitat. Hi ha dues alternatives:

- A través d'una aplicació instal·lada prèviament a l'equip.
- Mitjançant una funcionalitat inclosa al procés general de l'Administració Pública o entitat privada, de tal manera que no és necessari descarregar ni instal·lar cap aplicació específica.

La signatura electrònica estarà completa en aquest punt, però com a bona pràctica, el prestador del servei hauria d'oferir al ciutadà un justificant de recepció, per garantir al ciutadà la correcta

realització del tràmit administratiu corresponent. Per fer-ho, el prestador del servei genera un rebut per al tràmit realitzat, i el signa. Seguidament, una Tercera Part de confiança denominada Autoritat de Segell de Temps, signa aquest rebut garantint així el moment exacte en que s'ha acceptat el tràmit (ha de ser una entitat externa al prestador del servei, i reconeguda en l'àmbit de la legislació espanyola). Finalment, el rebut signat i segellat s'envia al ciutadà.

3.6 Autoritats de Certificació

En criptografia, una **Autoritat de Certificació** és una **entitat de confiança encarregada de la emissió i revocació de certificats digitals emprats per a la signatura digital amb criptosistemes de clau pública**. És, per tant, una entitat que legitima davant de terceres persones que accepten els seus certificats, la relació entre la identitat d'una persona i la seva clau pública. Aquest servei està basat doncs, en la confiança que els usuaris dipositen en l'Autoritat de Certificació, però no hi ha un procediment estàndard per demostrar que una Autoritat Certificadora mereix aquesta confiança. A nivell jurídic, és un cas particular dels Prestadors de Serveis de Certificació.

El funcionament és el següent. L'**Autoritat de Certificació** ha de **verificar la identitat** de la persona o entitat que requereix el certificat. És possible que aquesta comprovació sigui realitzada per la mateixa Autoritat de Certificació, tot i que, en determinats casos, com en el del DNIe, aquesta comprovació es farà de forma externa, mitjançant una **Autoritat de Registre** externa, que serà qui mantingui la informació sobre les identitats dels possibles demandants dels certificats digitals. Si ja s'han expedits els certificats a un determinat demandant, i tenen la condició de revocats, s'elimina aquesta revocació al realitzar la comprovació d'identitat.

Els certificats seran documents digitals que contenen informació del titular, i la clau pública d'aquest. Aniran signats per la Autoritat Certificadora amb la clau privada del titular (però aquesta clau no anirà inclosa en el certificat, donat que és privada). Els certificats revocats no són vàlids malgrat que siguin utilitzats durant el seu període de vigència. Un certificat pot ser que es trobi en condició de suspès. Això vol dir que la seva vigència es pot restablir en determinades condicions.

Per a sol·licitar un certificat de servidor web a una Autoritat de Certificació, una persona o entitat sol·licitant emplena una sèrie de dades que la identificaran utilitzant funcions de software del servidor web específiques per aquesta tasca. Entre aquestes dades s'inclourà el localitzador URL del servidor, i es generarà un parell de claus pública/privada. Amb totes aquestes dades, el software del servidor web composa un document que contindrà una petició CSR(Certificate Signing Request) en format PKCS#10 (PKCS correspon a una sèrie d'especificacions d'estàndards “de facto” denominades conjuntament com a Public-Key Criptography Standards), amb la clau pública inclosa, que serà enviat a la Autoritat de Certificació. Aquesta verificarà, ja sigui per si mateixa, o consultat una Autoritat de Registre, la informació aportada i el pagament. Si tot és correcte, s'enviarà al sol·licitant el certificat signat, que instal·larà en el seu servidor web amb les eines amb les que va crear el missatge de petició del certificat a la AC.

La pregunta següent serà, doncs, **com es pot estar segur que una Autoritat Certificadora és de confiança?** La resposta vindrà donada per la **jerarquia de certificació**. Les AC's disposen de certificats públics dels que en són titulars, i empren la clau privada associada per signar els certificats que emeten. En el cas que l'**Autoritat Certificadora** en qüestió ja **no tingui cap altra AC en un rang superior**, s'haurà de confiar en ella mitjançant la **confiança en les lleis dels diferents països, que atorgaran legalitat a les entitats anomenades Autoritats de Certificació Arrel**. Aquestes auto-signaran els seus certificats, convertint-los en l'element inicial de qualsevol

jerarquia de certificació. Aquestes estructures jeràrquiques estaran composades per diferents AC's sempre partint d'una **AC Arrel**, i en qualsevol dels nivells hi haurà una o varies d'aquestes Autoritats que podran signar certificats d'entitat final (titular de certificat, ja sigui servidor web, persona, o aplicació software) o bé certificats d'altres AC's subordinades que estiguin plenament identificades i que tinguin Polítiques de Certificació compatibles amb les dels rangs superiors.

Per establir l'esmentada confiança en les Autoritats de Certificació, el que es fa més comunament és instal·lar, mitjançant un fitxer creat a tal efecte, un certificat autosignat per la AC en qüestió, que serà l'arrel de la jerarquia en la que es vol confiar. Aquest certificat arrel ha de ser importat pels diferents navegadors instal·lats a l'equip. Si un certificat arrel d'una determinada Autoritat de Certificació es troba instal·lat en un navegador, qualsevol certificat signat per aquesta AC podrà ser validat, ja que es disposa de la clau pública amb la que verificar la signatura del certificat. Si a més el model de AC inclou una jerarquia, s'ha d'establir explícitament la confiança en els certificats de totes les cadenes de certificació en les quals es confia. És possible que un certificat contingui directament tota la cadena de certificació necessària per a ser instal·lat amb confiança, però, si no és el cas, es poden trobar aquests certificats a Internet mitjançant diversos mitjans de publicació.

Una Autoritat de Certificació pot ser pública o bé privada. El certificats arrel de les AC's Públiques, són reconeguts com a certificats de confiança en funció de la normativa dels diferents països, independentment d'estar o no instal·lats al navegador. Les AC's Públiques emeten certificats per a la població en general, a vegades dirigides a un conjunt de població concret, i poden signar AC's d'altres organitzacions.

La gestió dels certificats signats també queda al càrrec de les Autoritats de Certificació. Per tant, són les responsables de gestionar les revocacions dels certificats, tant les demandades pels usuaris, com per tercers legítims. Per dur a terme aquesta tasca fan servir les anomenades Certificate Revocation List , CRL, que emmagatzemen la informació sobre l'estat dels certificats caducats o revocats. És responsabilitat de les AC's publicar i actualitzar aquesta llista de forma eficient, i oferir les funcionalitats necessàries per a la renovació de la vigència dels certificats.

Donat que una AC pot emetre molts certificats, les CRL's poden arribar a tenir mides molt grans, fent poc eficient la seva descàrrega per part dels “tercers que confien”. Per solucionar aquesta problemàtica, les Autoritats de Certificació han creat mètodes alternatius de consulta de l'estat dels certificats, com servidors basats en protocols OCSP(Online Certificate Status Protocol) i SCVP (Server Based Certificate Validation).

Els certificats de ”entitat final” es poden dividir en dos tipus: certificats qualificats, quan designen a persones, o bé els que identifiquen servidors web, que es faran servir dins del protocol SSL aconseguint d'aquesta manera unes comunicacions xifrades segures amb l'esmentat servidor.

En el cas concret del DNIe, les funcions de l'**Autoritat de Validació**(encarregada de comprovar la validesa i vigència dels certificats electrònics continguts al DNIe) es divideixen en l'**Autoritat de Registre** (s'encarrega de registrar les dades identificatives dels ciutadans i entitats als quals s'atorgaran certificats) i l'**Autoritat de Certificació** (s'encarrega del control de la vigència dels certificats emesos). D'aquesta manera s'aconsegueix aïllar la comprovació de la vigència del certificat, de les dades identificadores del seu titular. Aquesta divisió dòna més transparència al sistema.

L'Autoritat de certificació per al DNIe es composarà de:

- La AC arrel, és a dir, Autoritat Certificadora de primer nivell, que només emetrà certificats per a sí mateixa, i per a les seves AC's subordinades,
- Les AC's subordinades, que seran les encarregades d'emetre els certificats als titulars del

DNIe. És la Direcció General de la Policia, Ministeri d'Interior, qui actua com a Autoritat de Certificació Arrel.

Els certificats que emet compleixen una sèrie de requeriments establerts per la normativa de la Direcció General de la Policia, relacionant dos parells de claus amb un ciutadà concret. No tenen accés a les transaccions realitzades amb els certificats que emeten.

L'**Autoritat de Validació** queda en mans de dos prestadors, més un tercer addicional:

- **La Fabrica Nacional de Moneda i Timbre**, més concretament la Reial Casa de la Moneda, donarà un servei de validació de caràcter universal a ciutadans, empreses i a les diferents Administracions Públiques.
- El **Ministeri d'Hisenda i Administracions Públiques**, que donarà servei de validació al conjunt de les Administracions Públiques.
- Addicionalment, i en un proper, la Entitat Pública Empresarial **Red.es** podria prestar serveis de validació.

La informació sobre els certificats electrònics revocats és emmagatzemada a les denominades llistes de revocació de certificats(CRL). El protocol emprat per a la prestació dels serveis de validació és el Online Certificate Status Protocol (OCSP). En la pràctica, un client OCSP envia una petició sobre l'estat d'un determinat certificat a l'autoritat de Validació, i aquesta, després de la pertinent consulta a les seves bases de dades CRL, retorna la resposta sobre l'estat del certificat via http. Aquest servei de validació està disponible de forma ininterrompuda durant tots els dies de l'any.

3.7 Certificats digitals

Un **certificat digital** és un **document emès i signat per una Autoritat Certificadora** (AC) que identifica la clau pública amb el seu propietari. Cada certificat està identificat de forma unívoca i té un període de validesa consignat en el propi document. Un **certificat permet validar la identitat de l'altre extrem d'una comunicació**, ja sigui una persona, una entitat o un dispositiu.

Com s'ha comentat anteriorment, una Autoritat Certificadora és una entitat de confiança de l'emissor i receptor d'una comunicació. Aquesta confiança d'ambdós en una 'tercera part de confiança' (trusted third party) permet que qualsevol dels dos confiï a la vegada en els documents signats per l'altre extrem de la comunicació. Si un certificat és autèntic i confiem en l'autoritat certificadora, podem confiar que el subjecte identificat al Certificat Digital es troba en possessió de la clau pública que s'assenyala en l'esmentat certificat. Així, si aquest subjecte signa un document i envia annex el seu certificat digital, qualsevol receptor que conegui la clau pública del subjecte (gràcies a la confiança que ens dóna la Autoritat de Certificació) podrà autenticar el document.

Els **certificats presents al DNIe** compleixen l'**estàndard x.509**. Aquest es refereix a l'estàndard criptogràfic per a infraestructures de clau púbica, una de les parts del conjunt d'estàndards de xarxes d'ordinador X.500 de la UIT-T . La UIT és la Unió Internacional de Telecomunicacions (ITU, en les seves sigles en anglès), òrgan especialitzat de la Organització de les Nacions Unides, encarregat de regular les telecomunicacions a nivell internacional entre les diferents administracions i empreses operadores. Està composada per tres divisions principals, la UIT-R, Sector referit a la Normalització de les Radiocomunicacions, la UIT-D, sector dedicat al Desenvolupament de les Telecomunicacions, i l'esmentada UIT-T, sector dedicat a l'estandardització i Normalització de les tecnologies de la comunicació i de la informació.

La primera versió de la x.509 va aparèixer l'any 1988, i fou publicada com el format x.509v1, essent, per tant, la més antiga proposta per a la infraestructura de clau pública (PKI) a nivell mundial. La seva antiguitat, unida al seu origen ISO/ITU, fa que sigui el PKI més estès. Es basa en un **sistema jeràrquic estricte d'Autoritats de Certificació** (AC's) per a l'emissió de certificats. Per tant, contrasta amb els models de xarxes de confiança, com PGP, on qualsevol dels nodes (i no només les AC's) té la capacitat de signar claus públiques, i per tant validar certificats d'altres. A l'any 93 va aparèixer la versió 2, que afegia dos nous camps, identificant de forma única a l'emissor i usuari del certificat.

Aquestes primeres versions de X.500 i X.509 van ser dissenyades a mitjans dels 80 i principis del 90, just abans del enorme creixement d'usuaris d'Internet. Per aquest motiu van ser dissenyat per al seu ús en entorns en que els ordinadors només s'interconnectaven entre ells de forma intermitent. Les CRL's que s'empraven a les versions 1 i 2 de X.509 eren molt simples, i generaven problemes en entorns d'Internet.

La **versió 3** defineix el **format de les extensions del certificat** emprat per emmagatzemar informació addicional del titular, així com la forma en que s'utilitza. Inclou, a més, la possibilitat de suport d'altres tecnologies com bridges i malles. Pot ser utilitzada en una web de confiança peer to peer de tipus OpenPGP, però des del 2004 s'utilitza d'aquesta manera en molt rares ocasions.

Aquesta versió és l'**estàndard internacionalment** acceptat per a certificats digitals. Es van introduir canvis significatius, el més important dels quals fou fer el format dels certificats i dels CRL's extensibles. D'aquesta manera no cal aplicar restriccions sobre l'estructura de la Autoritat de Certificació, donada la possibilitat de definir les seves pròpies extensions de certificats. Aquestes extensions permeten a l'organització emmagatzemar informació específica dins del seu entorn d'operació. Els camps o elements que formen part del format d'un certificat X.509v3 són els

següents:

- **Versió**: Aquest camp conté el número de versió del certificat codificat. Els valors que accepta són 1, 2 i 3.
- **Número de sèrie del certificat**: aquest camp és un sencer que assigna l'Autoritat de Certificació. Cadascun d'aquests números assignats per una A.C. ha de ser únic. Aquests números es fan servir per a les CRL's, és a dir, les llistes de revocació de certificats.
- **Identificador de l'algoritme de signatura**: aquest camp identifica quin ha estat l'algoritme emprat per a la realització de la signatura del certificat x.509 (per exemple el RSA, o el DSA).
- **Nom de l'emissor**: aquest camp identifica l'Autoritat de Certificació que ha signat i emès el certificat.
- **Període de validesa**: aquest camp emmagatzema la informació referent al temps durant el qual el certificat serà vàlid, i per tant, el temps que la Autoritat de Certificació està obligada a mantenir la informació sobre el seu estat. Es divideix en una data inicial, a partir de la qual el document comença a ser vàlid, i una data final a després de la qual el certificat deixa de ser vàlid.
- **Nom del subjecte**: aquest camp identifica el propietari de la clau pública continguda en el camp següent. El nom ha de ser únic per a cada entitat certificada per una Autoritat de Certificació específica, però pot emetre més d'un certificat amb el mateix nom si és per a la mateixa entitat.
- **Clau pública del subjecte**: aquest camp conté la clau pública del subjecte titular del certificat, els seus paràmetres, i l'identificador de l'algoritme que està capacitat per a utilitzar aquest clau.
- **Identificador únic de l'emissor**: aquest és un camp opcional que dona la possibilitat de reutilitzar noms d'emissor.
- **Identificador únic de subjecte**: camp opcional que permet reutilitzar noms de subjecte.
- **Extensions**: les extensions X.509v3 proporcionen una forma d'associar informació addicional a subjectes, claus públiques... als camps d'extensió es composen de tres parts diferenciades:
  - Tipus d'extensió: és un identificador d'objecte que dóna la semàntica i el tipus d'informació (cadena de text, data o altres estructures de dades) per a un valor d'extensió.
  - Valor d'extensió: Aquest és un subcamp que conté el valor actual del camp.
  - Indicador d'importància: aquest és un flag que indica a una aplicació si és o no segur ignorar el camp d'extensió si no reconeix el tipus. Aquest indicador proporciona una manera d'implementar aplicacions que treballen de mode segur amb certificats, i evolucionen a mida que es van afegint noves extensions.

    El conjunt d'extensions estàndard acceptades per la UIT i ISO, es troben publicades en un apèndix al X.509v3:
  - Limitacions bàsiques: aquest camp indica si el subjecte és una Autoritat de Certificació, i el màxim nivell de profunditat d'un camí de certificació a que es pot arribar a través d'aquesta AC.

- Política de Certificació: aquest camp conté les condicions sota les quals es va emetre el certificat i el seu propòsit.
- Ús de la clau: aquest camp s'empra per restringir el propòsit de la clau pública certificada, indicant el seu propòsit. Per exemple, indicar que només s'emprarà per signar, per a xifrar claus o bé per a xifrar dades. Aquest camp és important, i se sol marcar com a tal, donat que una clau específica té un propòsit concret, i emprar-la per a un altre seria invàlid.

El format X.509 de certificats s'especifica en un sistema de notació denominat Sintaxi Abstracta 1 (Abstract Sintax One o ASN-1). Per a la transmissió de dades s'aplica el DER(Distinguished Encoding Rules o Regles de Codificació Distingible), que transforma el certificat en format ASN-1 en una seqüència de bytes apta per a la seva transmissió en xarxes reals.

El estàndard X.509 permet tres mecanismes diferents per a la autenticació d'usuaris en una xarxa en processos de petició de serveis, missatges o enviament de la informació. El primer serà l'**autenticació a una via**, que implica només una transmissió. El segon l'**autenticació a dues vies**, que implica una transmissió i una resposta. La tercera serà l'**autenticació a tres vies**, que implica l'autenticació, la resposta, i el justificant de recepció d'aquesta.

3.8 Signatura electrònica

La signatura electrònica, com ja s'ha comentat en apartats anteriors, és una sèrie de dades que, a partir d'un missatge en clar, i associades a aquest, permeten la identificació del signant. Tant emissor com receptor poden identificar-se de forma mútua, evitant d'aquesta manera que terceres persones interceptin els missatges i alterin els seus continguts, i que alguna de les parts pugui “repudiar” la informació rebuda i inicialment acceptada.

Segons la Llei 59/2003 (Apèndix Llei 59/2003 sobre el DNI-electrònic) es defineixen tres tipus de signatura electrònica:

- **Signatura simple**: les dades poden ser utilitzades per a la **identificació** del signant (autenticitat).
- **Signatura avançada**: a més de la identificació del signant, ens dóna garantia de la **integritat** del document i de la clau utilitzada, detectant qualsevol canvi posterior. A més, permet vincular de manera única al signant i les dades signades, i aquesta signatura ha estat realitzada per mitjans que el signant pot mantenir sota el seu exclusiu control.
- **Signatura reconeguda**: és la signatura avançada, emparada per un certificat reconegut, és a dir, aquell que es dóna només a partir d'una **verificació presencial de la identitat del signant**. Permet, per tant, protegir la integritat dels documents electrònics signats, autenticar l'autor dels documents, i imputar a l'autor dels documents la qualitat d'autor dels mateixos.

Per a la realització de la signatura electrònica amb el DNIe existeixen nombroses funcions que poden ser emprades. Això es deu a que l'accés es fa a mòduls o capes intermitges de CSP i PKCS#11, proporcionant una interfície per a l'accés a la targeta estàndard.

És recomanable seguir els consell i conjunt de bones pràctiques presents a l'adreça web www.dnielectronico.es/Asi_es_el_dni_electronico/consejos.html.

Els mòduls que asseguren un funcionament correcte i segur del DNIe són el CSP i el PKCS#11. Aquests es poden descarregar de www.dnielectronico.es/descargas/ i contenen tot allò necessari per operar de forma segura amb el DNI-e, satisfent tots els requeriments de seguretat en quant a noves tecnologies que trobem al perfil de protecció CWA 14169.

3.9 Estàndards en criptografia

Els **PKCS (Public-Key Criptography Standars)** són els estàndards de criptografia creats i publicats pels laboratoris **RSA Security** de California. A aquests laboratoris se'ls hi van assignar drets de llicenciament per a la patent de l'algoritme de clau asimètrica RSA, i va adquirir els drets de llicenciament per a moltes altres patents de claus.

PKCS#1: Defineix el format del xifrat RSA.

PKCS#3:Estàndard d'intercanvi de claus Diffie-Hellman.

PKCS#5: Estàndard de xifrat basat en contrasenyes.

PKCS#7: Sintaxi del missatge criptogràfic (CMS).

PKCS#8: Sintaxi de la informació de clau privada.

PKCS#9: Tipus d'atributs seleccionats.

PKCS#10: Estàndard de sol·licitud de certificació (CSR).

PKCS#11:Interfície de dispositiu criptogràfic ("Cryptographic Token Interface" ocryptoki, HSM).

PKCS#12: Sintaxi d'intercanvi d'informació personal.

PKCS#13: Criptografia de corba el·líptica (en desenvolupament).

PKCS#14: Generació de números pseudo-aleatoris (en desenvolupament).

PKCS#15:Estàndard de format d'informació de dispositiu criptogràfic (DNIe)

4 Tecnologies emprades

El projecte ha estat realitzat sobre el sistema operatiu Linux, amb la seva distribució Ubuntu 12.04. Ha estat necessari configurar la Màquina Virtual de Java, la darrera versió emprada ha estat la 1.7.0_10. Per al desenvolupament de l'aplicació s'ha emprat Spring Source Toolsuite, versió 2.9.2.RELEASE, basada en Eclipse. Per al desplegament d'aplicacions s'ha fet servir Tomcat, en la versió 7. El motor de base de dades emprat ha estat MySql, versió 5.1. Per a la creació de la capa de persistència, enllaç de l'aplicació amb la base de dades, s'ha emprat la ORM Hibernate, en versió 3.2.0. Per l'accés al DNI-e, s'ha emprat el lector de Smart Cards C3PO LTC-31.

4.1 Costat del client

4.1.1 Applets

Un **Applet** és un petit programa, generalment escrit en **Java**, que forma part del context d'un altre programa, i que proporciona una **funcionalitat específica i clarament definida**. Els **Applets han de ser executats en un contenidor**, que els hi proporciona el programa amfitrió, mitjançant un plugin, o directament programes que suporten el model de programació per Applets.

Els **Applets** són emprats majoritàriament com a **components de pàgines web**, i s'utilitzen per donar **una funcionalitat a la pàgina**, que no seria possible amb HTML únicament. Els Applets de Java funcionaran correctament, **independentment de l'arquitectura de la màquina, navegador o sistema operatiu** en que s'estigui consultant una pàgina web. És per aquest motiu que els Applets de Java s'han convertit en una solució molt estesa per a la creació de funcions web. No poden executar-se de forma independent, si no que realitzen una funció molt específica, que potser no tindria sentit utilitzat de forma independent Com a exemples de funcionalitat dels Applets en pàgines web, podem esmentar:

- Funcions específiques, com càlculs matemàtics.
- Mostrar seqüències d'imatges i efectes visuals.
- Mostrar seqüències multimèdia amb efectes de so.
- Presentacions de gràfic interactius, que reaccionen als moviments fets amb el ratolí sobre el gràfic.
- Creació de diagrames i gràfiques.
- Petits jocs.

Per tant, poden proporcionar informació gràfica o bé interactuar amb l'usuari, normalment no tenen sessió, i els seus privilegis de seguretat són restringits. Entre els exemples més comuns, trobem les animacions en Flash, o els reproductors de vídeo capaços de mostrar vídeos incrustats en navegadors.

Un **Java Applet** és un codi Java que **no té un mètode main**, i que generalment s'utilitza per a realitzar tasques específiques en pàgines web. Un Applet de Java es pot executar a sobre de qualsevol navegador que suporti Java.

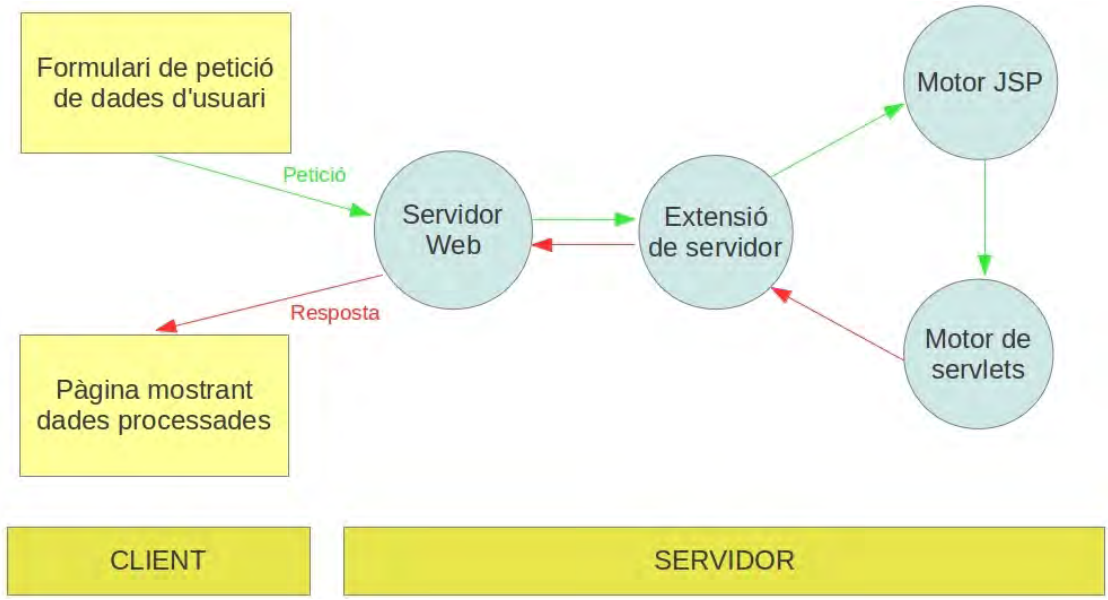
4.1.2 JSP

Java Server Pages (JSP) és una tecnologia que permet als desenvolupadors de software crear **pàgines web dinàmiques** de forma fàcil i ràpida, basades en **HTML, XML** i altres tipus de documents, i que són independents del servidor i de la plataforma on s'executen. Per desplegar i fer funcionar les pàgines web creades mitjançant JSP, és necessari un **servidor web compatible amb contenidors servlet**. En el nostre cas hem fet servir Apache Tomcat. El rendiment d'una pàgina JSP serà el mateix que tindria el servlet equivalent, donat que el codi és compilat de la mateixa forma que qualsevol altra classe Java. El fet que la màquina virtual de Java compili a codi màquina les parts de l'aplicació que ho requereixin, fa la tecnologia JSP més eficient que altres tecnologies web que executen el codi de forma purament interpretada.

JSP forma part de la família Java, un llenguatge de propòsit general, que no es limita únicament a la web. Amb Java és possible crear classes que s'encarreguin de la lògica de negoci i l'accés a les dades, i deixant **la part que genera el document HTML en fitxers JSP**. D'aquesta forma, **JSP separa les interfícies d'usuari de la de generació de contingut**, permetent que els dissenyadors puguin modificar la distribució de la pàgina sense preocupar-se de la lògica de negoci o comportament de l'aplicació.

JSP empra etiquetes XML per encapsular la lògica que genera el contingut d'una pàgina. La lògica de les aplicacions es troba en recursos de servidor (com a components de l'arquitectura JavaBeans) als que la pàgina accedeix amb les esmentades etiquetes. Tots els components amb format HTML o XML són enviats directament a la pàgina de resposta. El fet de **separar la lògica de la pàgina de la part de disseny fa més fàcil desenvolupar aplicacions web basades en Java**.

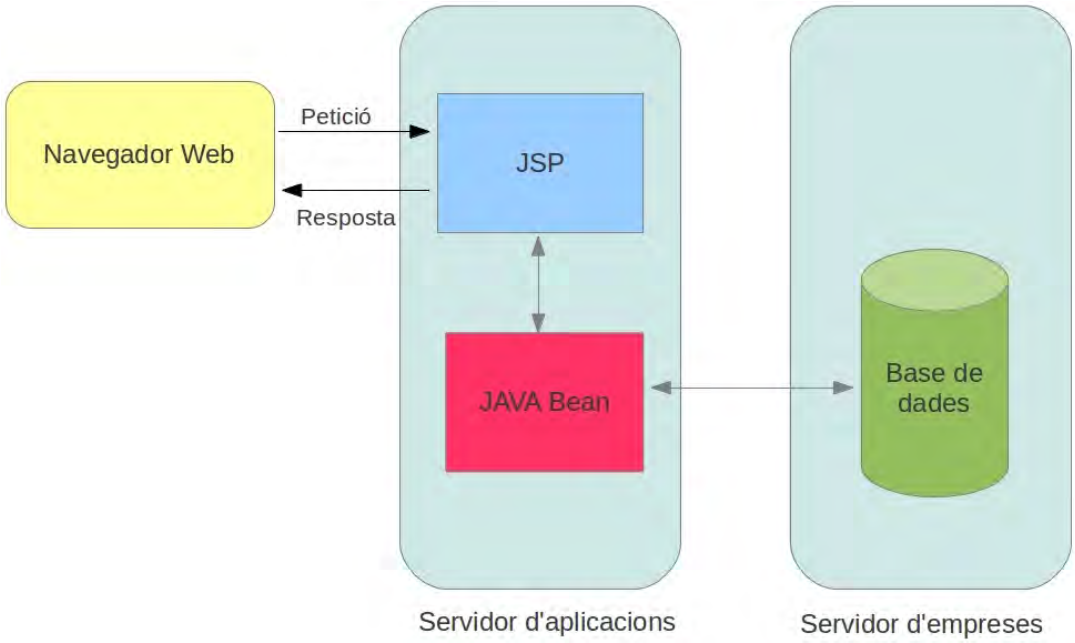
Els JSP i servlets permeten la creació de contingut dinàmic a les pàgines web, de forma similar a PHP, o els antics CGI's, però el fet que **s'executi a sobre de la màquina virtual de Java**, permet que **les aplicacions siguin independents de l'arquitectura de l'ordinador, el sistema operatiu o el navegador** en que es fan anar, sempre que existeixi una màquina virtual de Java disponible. Els **servlets només s'inicien una vegada**, iniciant un fil propi, i persistiran al servidor escoltant noves peticions, sense haver de perdre temps invocant-los de nou. Aquesta persistència permet que tasques com les sessions o les connexions a base de dades es facin de forma més eficient.



Il·lustració 23: Esquema de funcionament de la tecnologia JSP

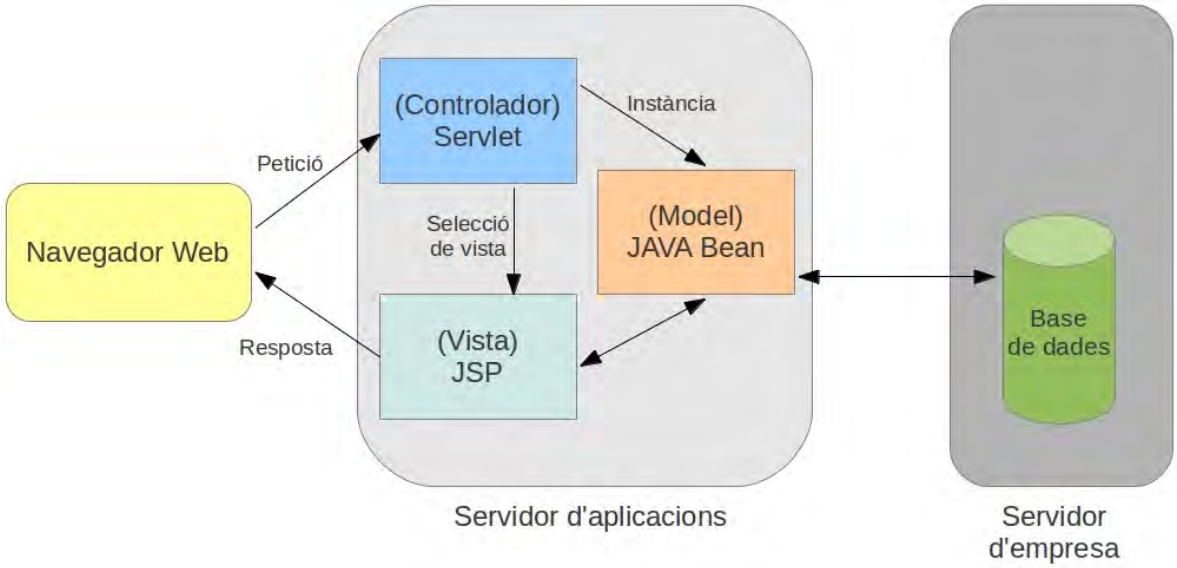
Els JSP són, en realitat, una forma de crear servlets. El codi JSP serà traduït a codi servlet pel motor JSP quan és invocat per primera vegada, i en endavant el que serà executat serà aquest codi servlet produint com a sortida el codi HTML que composa la pàgina web de resposta. Podem considerar JSP doncs, com una abstracció d'alt nivell dels servlets Java. Les Java Server Pages són traduïdes en temps real, i emmagatzemades en la caché de servlets per a la seva posterior reutilització. En aquest punt el servlet serà manegat pel motor de servlets, al igual que qualsevol altre servlet que no provingui d'una JSP. Serà aquest motor el que a partir d'ara carregarà la classe servlet, mitjançant un carregador de classes, i l'executarà per tal de crear el HTML dinàmic que serà enviat al navegador. **Aquest servlet continuarà donant servei des del servidor web, fins al moment en que la pàgina JSP es modificada**, cosa que implicarà una nova compilació a codi servlet. Els servlets són independents de la plataforma, i s'adapten perfectament a una infraestructura de servidor Web, ampliant les seves capacitats amb unes despeses mínimes per a manteniment i suport.

La tecnologia JSP presenta dos possibles vies per a la construcció d'aplicacions Web emprant les pàgines JSP. En el model d'arquitectura "**JSP Model 1**" (Il·lustració 24) la **pàgina JSP és l'encarregada de tramitar les sol·licituds i enviar les respostes als clients**.



Il·lustració 24: Model JSP 1

En el "**JSP Model 2**" (Il·lustració 25), s'integra l'ús dels servlets i les pàgines JSP. En aquest model, **les pàgines JSP s'utilitzen únicament en la capa de presentació**, i els **servlets per a les tasques de processament i la lògica de negoci**. Són **els servlets els que controlen el processament de les sol·licituds i la creació dels Beans necessaris per al funcionament de la pàgina JSP**. El servlet, a més, actua com a controlador responsable a quina pàgina transmetrà la sol·licitud. La pàgina JSP recupera els objectes creats pel servlet, i n'extreu el contingut dinàmic per inserir-lo a dins d'una plantilla.



Il·lustració 25: Model JSP 2

Aquest segon model promou l'ús de l'arquitectura **Model View Controller (MVC)**, per al qual s'han creat diversos frameworks que utilitzen aquest model de disseny, i que realment separen la capa de presentació de la de continguts.

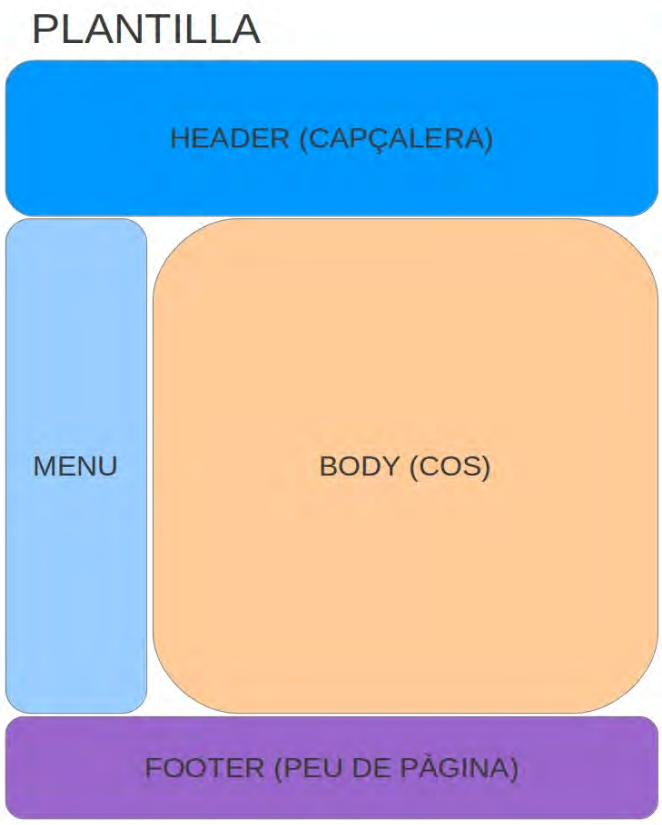
Per tant, **JSP** és una **atractiva alternativa** per a la programació de **pàgines web dinàmiques**,

donat que és independent de la plataforma en que s'executa, i produeix millores en el rendiment degut a la **separació per capes de les diferents parts de l'aplicació, la capa de presentació, la lògica de negoci, i la capa de persistència**. A més, JSP es pot escalar per a emprar en aplicacions empresarials de gran envergadura, ja que és fàcil d'administrar i, el més important, fàcil d'utilitzar.

Apache Tiles

A les pàgines JSP normalment hi trobarem una part central que serà la que tindrà el contingut dinàmic, i diferent a cada pàgina, i una sèrie de continguts, com la capçalera, el menú o el peu de pàgina, que seran iguals a totes les pàgines de l'aplicació. El codi d'aquestes parts s'haurà de copiar a totes les pàgines JSP per tal de mantenir el mateix format a tota l'aplicació.

Per tal d'evitar aquesta situació, va aparèixer Apache Tiles, un sistema de plantilles dissenyat i implementat per tal de facilitar el desenvolupament d'interfícies d'usuari de les aplicacions Web (Il·lustració 26). Tiles permet definir als autors de la pàgina fragments (tiles) que es poden muntar a la pàgina completa en temps d'execució. Aquests fragments es poden emprar tant per a reduir la duplicitat de codi , i per tant d'elements a la pàgina, o per crear unes plantilles que puguin ser reutilitzades en altres pàgines de l'aplicació, agilitzant el desenvolupament.



Il·lustració 26: Model de plantilla de Tiles

Inicialment, Tiles va sorgir com a component de l'IDE Struts, però donada la gran popularitat que va adquirir, finalment va ser extret, i integrat en molt altres Frameworks de creació d'aplicacions JSP.

Primerament s'ha d'instal·lar Tiles a la nostra aplicació. Al servidor Tomcat, el concepte d'instal·lació fa referència a la descàrrega de llibreries .jar, que seran col·locades a la carpeta WEB-INF/lib. També és possible que siguin posades a la carpeta lib del servidor, i que siguin compartides per totes les aplicacions disponibles.

Tiles haurà de ser configurat a l'aplicació per tal que pugui ser utilitzat. S'ha de modificar el fitxer web.xml, i crear un fitxer de definició de plantilles. Aquest fitxer contindrà dos parts: una plantilla o layout, i uns fragments o tiles, que composen la plantilla. D'aquesta forma, per al mateix layout es poden posar diferents fragments. Per exemple, una aplicació anomenada “myapp” té com a pàgina d'inici “myapp.homepage”, i utilitza com a plantilla “/layout/classic.jsp”. Aquesta plantilla utilitza “tiles/home_body.jsp” com a cos de la pàgina. Però en qualsevol moment es pot crear una nova definició, “myapp.nadal”, que empri la mateixa plantilla, però que posi com a body “/tiles/nadal.body.jsp”. D'aquesta manera reutilitzem parts del disseny com capçaleres, peus de pàgina o menús.

La gran diferència respecte al que podem aconseguir mitjançant la llibreria d'etiquetes <jsp:>, que apareix per defecte a la instal·lació de Tomcat, és que amb Tiles es poden niar definicions, emprar expressions, comodins, composició dinàmica, atorgant al desenvolupador moltes més possibilitats a l'hora de dissenyar una aplicació Web amb una interfície d'usuari estandarditzada, reutilitzant codi, i evitant així la duplicitat d'elements.

4.1.3 Smart Cards i lectors

Il·lustració 27: Lector de Smart Cards C3PO LTC-31

Una **Smart Card**, o targeta intel·ligent és una targeta de plàstic que conté un **microxip** d'ordinador **integrat**. Aquest microxip pot ser de dos tipus:

- Les **targetes de memòria**, que contenen únicament components de memòria no volàtil, i possiblement una lògica de seguretat.
- Les **targetes microprocessador**, les quals, a més de components de memòria, contenen un processador per fer tractament de les dades. Aquestes dades són guardades i/o processades dins del propi xip de la targeta.

L'accés a les dades es fa a través d'un lector de targetes (Il·lustració 27), que a més els hi subministrarà energia, ja que les targetes no con contenen bateries. Aquest tipus de targetes es fan servir avui dia en multitud de camps, com la identificació sanitària, les transaccions bancàries o l'ús de transports públics, i estan passant per davant d'altres tecnologies com els codis de barres o les bandes magnètiques.

Les Smart Cards van ser inventades i patentades durant la dècada dels 70, però hi ha discussions sobre l'inventor original, entre els que es troben Juergen Dethloff d'Alemanya, Kunitaka Arimura de Japó i Roland Moreno de França. El que si està clar és que el primer ús massiu d'aquesta tecnologia va ser pel pagament de la telefonia pública a França l'any 1983, en un intent per evitar els robatoris. Des de llavors, l'ús d'aquestes targetes s'ha estès en diversos àmbits. S'ha de destacar la publicació al 1996 i posterior revisió a l'any 2000 de l'**estàndard EMV**(per les inicials dels noms de les principals empreses que el van promoure, Europay, Mastercard i Visa) **per a la interoperabilitat de pagament amb targeta intel·ligent**. L'ús en aquest camp de les Smart Card millora la seguretat que aportaven tecnologies anteriors, sobretot en quant a protecció de les dades i en comunicacions a través d'Internet. Aquest estàndard ha anat imposant-se poc a poc a la banda magnètica, tot i que els costos de la seva implementació fan pensar que en breu podrien ser substituïts per altres tecnologies més econòmiques.

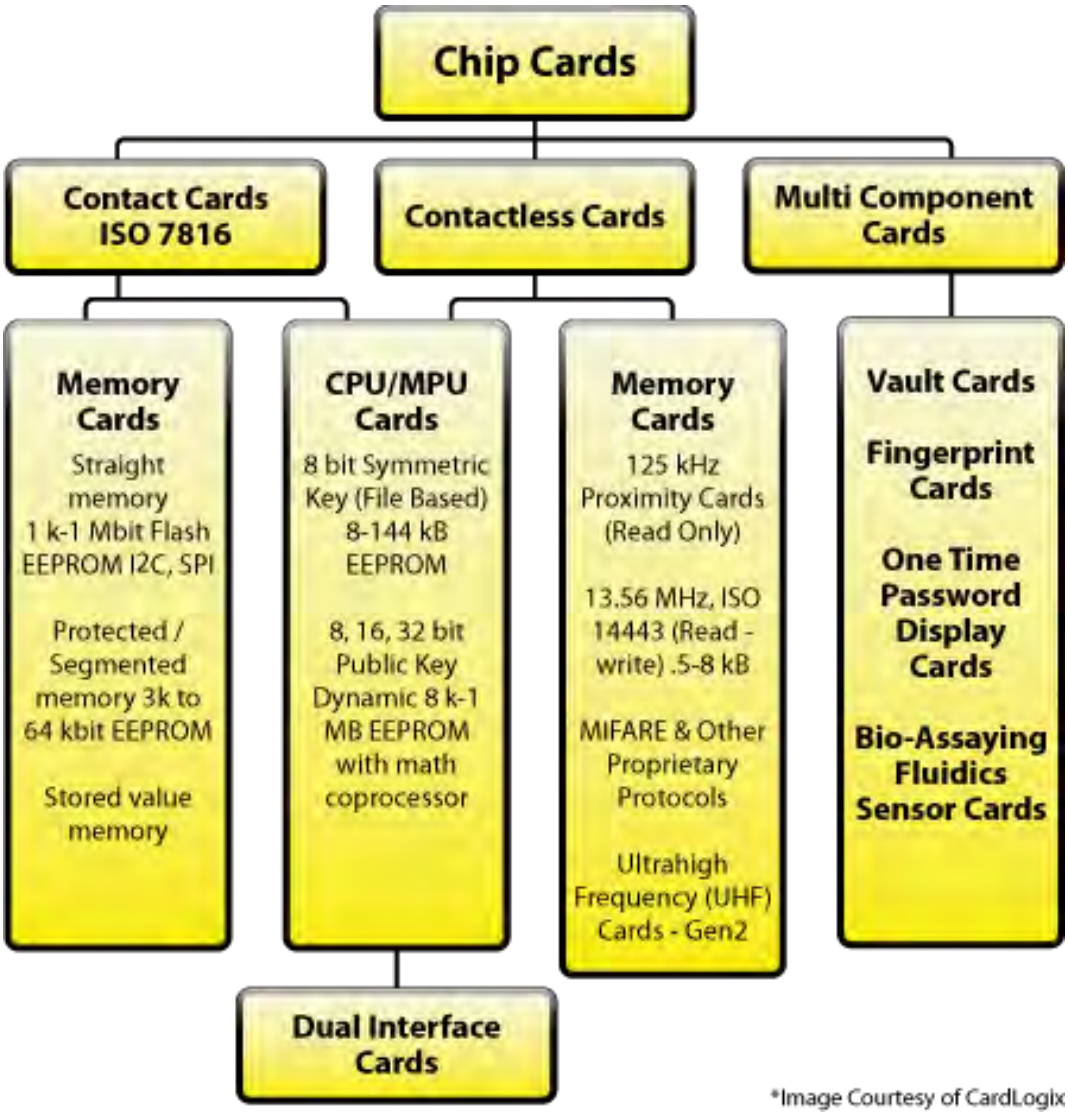
Les targetes intel·ligents també s'estan utilitzant per a la **identificació de persones**. Moltes empreses identifiquen als seus treballadors amb targetes d'aquest tipus. També, a nivell governamental, molts països utilitzen aquesta tecnologia per a la identificació de ciutadans, i inclús determinats països, com Malàisia, empren una targeta multipropòsit, mitjançant la qual s'aconsegueix la identificació personal, la llicència de conduir, la targeta de l'assegurança, el pagament de transport públic i la identificació del viatger amb una única targeta.

Però l'aplicació amb l'ús més estès d'aquesta tecnologia han estat les **Subscriber Identity Modules**, les conegudes targetes **SIM** necessàries per al funcionament de qualsevol dispositiu que faci ús de les xarxes de **telefonia mòbil** sota la Global System for Mobile Comunication (GSM) estàndard. Cada dispositiu ha de disposar d'un identificador únic, emmagatzemat a la SIM, que s'encarrega de l'administració del privilegis de cadascun del subscriptors. La meitat de les Smart Cards que es fabriquen cada any, són destinades a aquest camp.

Existeixen molts altres usos de les Smart Cards, el comerç electrònic, incloent les targetes dels comerços per fidelitzar clients; les targetes d'identificació sanitària, que fan possible la identificació d'un pacient de forma ràpida i inequívoca; o bé l'accés físic a determinats edificis o sales, mitjançant la identificació amb targeta intel·ligent. Tots aquests camps empren Smart Cards degut a la facilitat d'ús d'aquesta tecnologia, i a les millores de seguretat que introdueix. La possibilitat de falsificació de les dades de l'usuari contingudes a la targeta és molt més baixa que amb altres tecnologies com ara les bandes magnètiques o els codis de barres. A més, el manteniment de les targetes i els lectors necessaris per la implementació de l'ús d'aquesta tecnologia s'ha demostrat més econòmic que altres

solucions. A més, són robustes enfront un gran ventall d'amenaces informàtiques, des de l'intent de captura del login i password, fins a atacs més sofisticats com el de “Man in the Middle”, o trojans.

Tipus de Smart Cards



Il·lustració 28: Tipus de Smart Cards

Les Smart Cards es construeixen a partir de diferents capes de materials disposats en substrats, i que donen lloc a una targeta d'una vida útil determinada. Avui dia, típicament es construeixen amb PVC, polièster o policarbonat. S'afegeix després el xip a la targeta i les dades que porta impreses. Tot i que de cara a l'usuari sembla un element simple, poden haver materials de 12 tipus diferents.

Les Smart Cards es poden classificar de diferents formes (Il·lustració 28): pel format, per les capacitats, per l'estructura del sistema operatiu, o pel tipus d'interfície.

Pel format trobem:

– **ID000**: el de les targetes SIM de telefonia mòbil i de les SAM (Security Access Module) per

autenticació criptogràfica mútua de targeta i terminal.

- **ID00**: mida intermitja poc emprada comercialment.
- **ID1**: el més habitual, de la mida de la targeta de crèdit.

Per les capacitats es divideixen en:

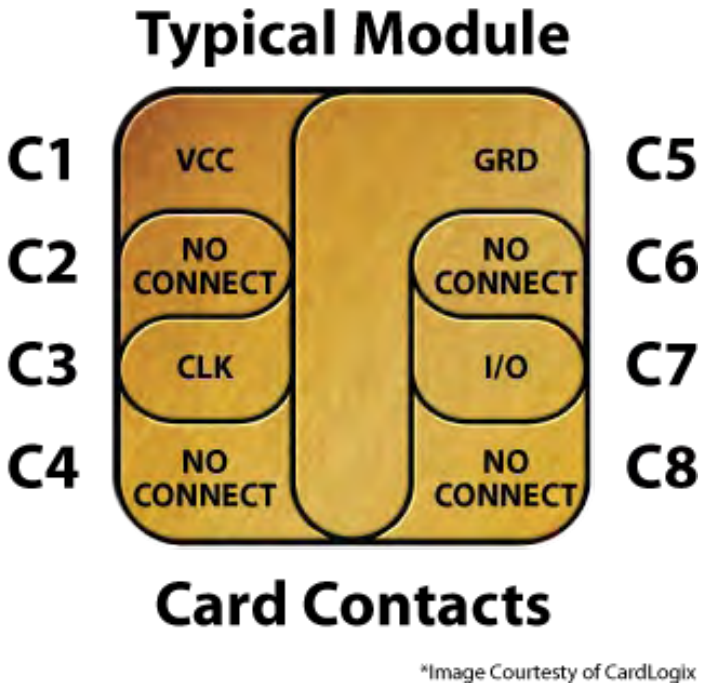
- **Targetes de memòria**: Les que emmagatzemen dades, però no contenen cap aplicació executable. Solen emprar-se per a tasques d'identificació, però en entorns de baix requeriment de seguretat.
- **Targetes microprocessades**: la seva estructura és anàloga a la d'un ordinador (processador, memòria volàtil i memòria persistent). Emmagatzemen dades i aplicacions, i se solen emprar per a identificació, i pagament amb moneders electrònics.
- **Targetes criptogràfiques**: són targetes microprocessades que inclouen mòduls per a la execució d'algoritmes de xifrat i signatura digital i que poden emmagatzemar de forma segura certificats digitals i clau privada necessaris per a l'execució dels mateixos. A més, permeten l'autenticació sense que el certificat surti de la targeta donat que el propi processador de la targeta realitza la signatura.

Segons la estructura del sistema operatiu, les Smart Card es poden classificar en:

- **Targetes de memòria**: són simplement un contenidor de fitxers, sense aplicacions executables. El seu sistema operatiu doncs, és limitat, ja que disposen d'una sèrie de comandes molt bàsiques per a la lectura i escriptura de les seccions de memòria. Poden tenir capacitats de seguretat en determinades zones de memòria.
- **Basades en sistemes de fitxers, aplicacions i comandes**: disposen de l'equivalent del sistema de fitxers descrit a l'estàndard ISO/IEC 7816 part 4, i un sistema operatiu que conté aplicacions (comandes) que es poden cridar a través de API's de programació.
- **Java Cards**: contenen i són capaces d'executar mini-aplicacions Java. El seu sistema operatiu és una petita màquina virtual de Java, i es poden carregar dinàmicament aplicacions desenvolupades específicament per a aquest entorn.

Segons la seva interfície, les Smart Card es poden dividir en:

- **De contacte**: les més habituals, disposen d'uns contactes metàl·lics visibles que segueixen un estàndard, i que seran utilitzats mitjançant el lector de targetes. Per aquest contactes rebrà alimentació i dades (Il·lustració 29).



Il·lustració 29: Contactes Smart Card

Els estàndards ISO/IEC 7816 i ISO/IEC 7810 defineixen:

- La forma física (part 1).
- Posició de les formes dels connectors elèctrics (part 2).
- Les característiques elèctriques (part 3).
- Format de les comandes (ADPU's) enviats a la targeta i les respostes retornades per la mateixa.
- La duresa de la targeta.
- La funcionalitat.

Els lectors de les targetes intel·ligents de contacte s'empren per la comunicació entre la targeta i un amfitrió, per exemple un equip informàtic.

– **Sense Contacte**: en aquest tipus de targeta la comunicació es produeix sense contacte físic entre el dispositiu i la targeta. Aquesta conté etiquetes RFID (Radio Frequency Identification, Identificació per Radiofreqüència) i la comunicació es realitza mitjançant inducció. L'estàndard és el ISO/IEC 14443 i els tipus existents permeten la comunicació fins a 10 cms. Es treballa en nous estàndards que augmenten aquesta distància.

– **Híbrides**: són targetes sense contacte, però que contenen un segon xip, aquest sí, de contacte. Ambdós poden ser de memòria o microprocessadors, i normalment s'empra la part sense contacte per a tasques de transacció ràpida, com els transports, i la de contacte per transaccions més crítiques, com les bancàries.

El DNIe és una targeta de contacte amb microprocessador que segueix la ISO 7816 i de format físic ID1 (de la mida de les targetes de crèdit). Per a la seva interacció amb l'equip informàtic, s'ha fet servir un lector de Smart Cards recomanat especialment per a l'ús amb DNI electrònic espanyol. Es tracta del C3PO LTC-31 (https://www.c3po.es/products-page/lectores-para-pc/ltc31-usb/) i aquí estan descrites les seves característiques segons indicacions de la pàgina web del producte:

- Característiques físiques:
  - Disseny de reduïdes dimensions i poc pes que facilita la seva portabilitat.
  - Base plana per a la seva correcta subjecció a altres dispositius com teclat o monitor.
  - Carcassa de PVC lleuger i resistent.
- Característiques tècniques:
  - Interfície USB 2.0.
  - Instal·lació Plug and Play per a Windows i Mac OS.
  - Actualització de firmware in-site.
  - CPU CMOS de 8 bits.
  - 2 Leds d'informació: un verd i un vermell.
  - Alimentació de 5V DC del propi ordinador.
  - Velocitats de comunicació de 9.600 bps fins a 1.500.000 bps.
- Sistemes operatius:
  - Sistemes Windows en Personal Computer.
  - GNU/Linux, MAC OS X, i altres sistemes de nucli UNIX suportats per libccid.
  - Altres drivers sota demanda.
- Targetes suportades:
  - DNI electrònic.
  - Targetes microprocessades amb protocols T=0 i T=1 (EMV, Targeta criptogfica, CERES, StarCos, JavaCard...)
  - Targetes de memòria amb protocols S=8, S=9, S=10 (SLE5542 (C3P2K), SLE4442, SLE4432 i SLE4428).
- Especificacions suportades:
  - PC/SC (Personal Computer / Samrt Card).
  - ISO 7816 per a targetes xip.
  - CSP (Cryptographic Service Provider) i API PKCS#11.
  - Especificacions EMV Nivell 1.
  - USB CCID (Chip Card Interface Device).

Per tal de fer funcionar el DNIe a través del lector de Smart Cards C3PO LTC-31 en distribucions Linux, i més concretament en Ubuntu, distribució emprada per la creació i provatures de la nostra aplicació, és necessària la instal·lació de **OpenSC**. **OpenSC** és un conjunt de llibreries i utilitats que permeten la operativitat amb Smart Cards. La seva orientació principal és el suport per a operacions criptogràfiques, i facilitar el seu ús en aplicacions de seguretat, com poden ser l'autenticació, la encriptació d'informació o la signatura digital. Les llibreries **OpenSC** implementen la API estàndard **PKCS#11**, de forma que les aplicacions que suporten aquest estàndard, com navegadors (Firefox) o clients de correu electrònic (Thunderbird) el poden utilitzar. En la targeta OpenSC s'implementa el estàndard PKCS#15, i aquest el farà compatible amb qualsevol software/targeta que també el suporti.

OpenSC ha estat desenvolupat per un equip de voluntaris internacionals, i la seva llicència és **Open Source**, sota la llicència **LGPL** en la seva versió 2.1 i les posteriors. La darrera versió estable publicada és la Open SC 0.13.0, que va ser presentada el 4 de Desembre de 2012.

El DNIe basa el seu funcionament en un plugin de OpenSC, del qual, al principi, no es disposava del codi font, donat que la Direcció General de la Policia i Guàrdia Civil no el van voler publicar. Per aquest motiu, de de OpenSC va decidir que no facilitaria la carrega de plugins, donat el desconeixement existent del codi font d'aquestos plugins, cosa difícilment justificable quan ens estem referint a llicències lliures i de codi obert. Aquesta decisió significava la sentència de mort del nou DNI electrònic en Linux.

Però finalment, i amb total desconeixement dels motius reals que van provocar aquesta decisió, la Direcció General de la Policia i Guàrdia Civil van publicar el codi font del plugin, però amb una llicencia de copyright que impedia utilitzar-lo. Posteriorment sí van publica un “manual” per programar el DNIe, obrint la possibilitat a la integració del DNIe en OpenSC.

Un treballador de l'Administració Pública, **Juan Antonio Martínez**, amb nickname jonsito a kriptopolis.org, va decidir dur a terme aquesta integració, creant un driver de codi obert per a l'ús del DNI electrònic en entorns Linux. Aquest driver fou escrit des de zero, i sota llicència LGPL lliure, i totalment compatible amb el projecte OpenSC, per a ser integrat al mateix.

Aquest driver ha estat testejat i verificat amb èxit, i compta amb l'aprovació tant de la Direcció General de la Policia, com del projecte OpenSC.

4.1.4 Javascript

Javascript és un llenguatge de programació que s'utilitza, principalment, al costat del client **implementat a sobre de navegadors web**, per tal de donar millores a la interfície d'usuari, i per **crear continguts dinàmics** a les pàgines que l'utilitzen. Pot ser emprat també en altres tipus d'aplicacions fora del web, com ara aplicacions d'escriptori, o inclús en documents pdf, però no en un ús tan massiu. També existeix una versió per al costat de servidor, anomenada SSJS (Server Side JavaScript).

Desenvolupat originàriament per **Brendan Eich, de Netscape**, el seu nom original era Mocha. Més tard va ser reanomenat com LiveScript, i finalment va passar a anomenar-se JavaScript, en un anunci conjunt amb Sun Microsystems, coincidint aproximadament amb el moment en que Netscape Navigator, el navegador més important de la època, va agregar suport per a la incipient tecnologia Java, al Desembre de 1995. El canvi de nom va generar confusió, ja que molta gent va pensar que JavaScript era una mena de prolongació de Java, però més aviat va ser una estratègia de Netscape per guanyar prestigi i capacitat d'innovació en el camp dels llenguatges de programació web, aprofitant l'aliatge amb Sun Microsystems.

Javascript és un llenguatge de programació **interpretat**, és a dir, **no requereix compilació**. Té una sintaxi similar a C, però amb noms i convencions més properes a Java. A diferència d'aquest, no és un llenguatge orientat a objectes pròpiament, ja que no disposa d'herència, si no més aviat un llenguatge basat en prototips, donat que les noves classes es generen clonant les classes base (prototips) i estenent la seva funcionalitat.

L'any 1997, els autors van proposar JavaScript per a que fos **adoptat com l'estàndard de la European Computer Manufacturer's Association, ECMA**, que, a pesar del seu nom, és una institució no només europea, si no internacional, amb seu a Ginebra. Al Juny de 1997 fou adoptat com a estàndard ECMA,rebent el nom de ECMAScript, i posteriorment, també fou designat com a estàndard ISO.

Microsoft va crear la seva implementació del ECMAScript, anomenat Jscript. Va ser adoptat en la versió 3.0 d'Internet Explorer, i alliberat a l'agost de 1996. La seva principal novetat va ser la compatibilitat amb l'efecte 2000 a les funcions de data. És tan similar a JavaScript, que sovint es confonen, i inclús s'empren indistintament, però, en molts aspectes, Jscript és incompatible amb la de ECMA.

Per tal d'evitar aquestes incompatibilitats, el **World Wide Web Consortium** va dissenyar el **estàndard DOM (Document Object Model, o Model de Objectes del Document)**, que incorporaven Internet Explorer 6, Netscape Navigator 6, Opera 7, i Mozilla des de la seva primera versió.

JavaScript s'ha convertit en un dels llenguatges de programació més populars a Internet, tot i les reticències inicials de molts programadors, donat que estava més orientat a publicadors d'articles o aficionats, i no a programadors. L'arribada d'**Ajax (Asynchronous JavaScript And XML)** ha retornat JavaScript a l'escenari, atraient l'atenció de molts programadors. Per aquest motiu, hi va haver una gran proliferació de frameworks i llibreries d'àmbit general, que han derivat en una millora de les pràctiques de programació amb JavaScript, i augmentant el seu ús fora de navegadors (exemple d'això va ser la publicació al 2009 de CommonsJS, projecte creat amb l'objectiu d'especificar una llibreria per a tasques d'ús comú principalment desenvolupades fora del navegador web).

La creació de funcions encastades a les pàgines HTML, i que interactuen amb el DOM

(Document Object Model) de la pàgina ens permeten realitzar diverses funcions dinàmiques amb les pàgines web. Alguns exemples d'ús són:

- Carregar nous continguts a la pàgina, o enviar les dades al servidor a través d'Ajax, sense necessitat de recarregar la pàgina completa (per exemple, a les xarxes socials, es poden enviar canvis d'estat sense sortir de la pàgina ni recarregar-la completament).
- Animacions d'elements de les pàgines, ja sigui per tal de fer-los desaparèixer, canviar les mides, colors, o moure'ls per la pantalla.
- Contingut interactiu, com jocs, àudio i vídeo.
- Validació de les dades d'entrada a un formulari web, per assegurar la validesa abans de ser enviades al servidor.
- Transmissió d'informació sobre els hàbits de navegació per fer personalitzacions, o bé anàlisis web.

El fet que **JavaScript** s'**executi localment al navegador del client**, en lloc d'un servidor remot, fa que el **rendiment millori**, ja que el navegador pot respondre més ràpidament a les accions de l'usuari. A més, JavaScript permet detectar accions que dugui a terme l'usuari, i que amb HTML pla, resultaria impossible, com ara les pulsacions de teclat. Aplicacions com diversos proveïdors de correu electrònic via web, com ara Gmail tenen la major part de la seva lògica d'interfície d'usuari escrita en JavaScript, enviant peticions al servidor, per exemple el contingut del missatge. La tendència actual a l'ús de Ajax explota de forma similar aquesta tècnica.

Avui dia, **JavaScript** és una marca registrada d'**Oracle Corporation**, i és utilitzada sota llicència pels productes creats per Netscape Communications, i entitats actuals com la Fundació Mozilla.

4.1.5 Sistema operatiu Ubuntu

Ubuntu (Il·lustració 30) és una **distribució del sistema operatiu Linux, basat en Debian**, i distribuït com a **software lliure i gratuït**, que inclou el seu propi entorn d'escriptori anomenat Unity, des de la versió 11.04. L'objectiu inicial era fer de Debian una **distribució més fàcil d'entendre i d'utilitzar pels usuaris finals**, corregint diversos errors d'aquest i facilitant certes tasques com ara la gestió de programes. Aquesta facilitat d'ús ha fet que, segon moltes estadístiques web, la quota de mercat d'Ubuntu entre les distribucions Linux, sigui d'aproximadament el 49%, i amb previsió d'augment en el futur. Inicialment va ser llençat el 20 d'Octubre de 2004.

Il·lustració 30: Logo de Ubuntu

Principalment **Ubuntu utilitza software lliure**, però hi ha certes excepcions, com determinats drivers privatius, a més de firmware i software no lliure, inclòs al kernel de Linux, i una part de software no lliure present en determinats repositoris separats dels lliures. Ubuntu empra, al igual que Debian, el **format de paquets .deb**, i les eines d'administració dels paquets APT, dpkg i alguns front-ends. A vegades, aquest paquets són compatibles en les dues distribucions a nivell binari, però en certs casos han de ser recompilats per ser funcionals en Ubuntu. A més de l'ús del mateix format de paquets, Ubuntu manté fortes unions amb la comunitat de Debian, contribuint en tots els canvis de forma directa i immediata. Molts dels desenvolupadors d'Ubuntu són els mateixos dels paquets més importants de la distribució Debian.
El patrocinador d'Ubuntu, **Canonical**, és una empresa britànica propietat del Sud-africà Mark Shuttleworth,, el qual ha donat suport econòmic des del principi al projecte, mitjançant els beneficis obtinguts de la venda de la seva empresa, Thawte, a VeriSign. El sistema operatiu s'ofereix als usuaris de forma gratuïta, i el **finançament es duu a terme mitjançant serveis vinculats al sistema operatiu, o amb suport tècnic**. El fet de mantenir-lo lliure, fa que molts desenvolupadors s'hagin implicat en la millora del projecte. Existeix una versió de servidor, anomenada Ubuntu Server; una versió empresarial, Ubuntu Bussines Desktop remix; una per a televisions, Ubuntu TV; i actualment es troba en fase de desenvolupament la versió per a telèfons mòbils intel·ligents, a més de la versió que corre a sobre d'Android, i que ja es troba al mercat.
Canonical presenta una nova versió d'Ubuntu cada sis mesos, i aquestes reben suport (mitjançant patches i actualitzacions) al llarg de 9 mesos, però cada 2 anys, apareix l'anomenada versió **LTS, Long Term Suport**, que rep **suport** per part de Canonical **durant 5 anys**.
Ubuntu suporta oficialment les arquitectures de 32 bits (x86) i les de 64 bits (x86 64) tant en ordinadors personals com en servidors, però extraoficialment ha estat portat a altres arquitectures com ARM, PowerPC o SPARC.
Els **usuaris** poden **contribuir en el desenvolupament d'Ubuntu**, escrivint codi, solucionant bugs, provant versions inestables o contribuint a la traducció de manera voluntària a través d'Internet. D'aquesta manera, s'ha aconseguit que Ubuntu estigui disponible en més de 130 idiomes.

Tot i que des de la versió 11.04, la interfície d'usuari ha deixat de ser GNOME, per començar a utilitzar Unity, de la pròpia Canonical, continua utilitzant el conjunt d'aplicacions GNOME. De totes formes, existeixen altres versions extraoficials, mantingudes per la comunitat. Entre el software inclòs per defecte a Ubuntu, trobem el navegador Firefox, el programa de missatgeria instantània Empathy, el client de correu Thunderbird, l'administrador d'arxius Nautilus, la suite ofimàtica LibreOffice entre molts altres.
Inclou, a més, funcions de seguretat avançades. Entre les seves polítiques s'inclou la no activació de forma predeterminada de processos latents en el moment d'instal·lar-se. Per aquest motiu no hi ha tallafocs predeterminat, donat que no hi ha cap servei que pugui atemptar contra la seguretat del sistema. Per a les tasques administratives per línia de comandes, empra l'eina anomenada “sudo” (Switch User do) evitant així la utilització de l'usuari administrador.
Internament, el **software d'Ubuntu es divideix en 4 seccions**, anomenades “components”, que separen els diferents tipus de llicències, i la prioritat amb que s'atenen els problemes reportats pels usuaris. Aquests components són:

- **Main**: conté únicament els paquets que compleixen els requisits de la llicència Ubuntu, els quals tenen suport disponible per part de l'equip de desenvolupament. Inclou tot el necessari per a la majoria de sistemes Linux d'ús general, i els paquets d'aquest component tenen garantida l'ajuda tècnica i les actualitzacions de seguretat necessàries.
- **Restricted**: conté els paquets més importants suportats pels desenvolupadors d'Ubuntu, però que no estan disponibles sota cap mena de llicència lliure per poder ser inclosos en el component main. Aquí trobem, per exemple, els drivers propietaris de diverses targetes gràfiques com ATI o Nvidia. No es pot garantir una ajuda tan immediata, donada la impossibilitat d'accedir al codi font.
- **Universe**: conté tots els programes, amb o sense llicència restringida, que, tot i no tenir suport per part d'Ubuntu, si el reben per part de la comunitat. Així es poden separar tota mena de programes a gust dels usuaris, però en un lloc diferent dels suportats per l'equip de desenvolupament.
- **Multiverse**: aquí trobem tots els paquets sense suport, perquè no compleixen els requisits del software lliure.

La versió actual d'**Ubuntu és la 13.04** (Raring Ringtail), tot i que pel desenvolupament de l'aplicació s'ha fet servir una de molt més antiga, la **11.10** (Oneiric Ocelot) per evitar problemes d'estabilitat amb les noves versions.

4.2 Costat del servidor

4.2.1 Java

Introducció

Durant l'any 1990, l'empresa **Sun Microsystems,** dedicada a la venda d'estacions de treball, servidors, components informàtics, software (sistemes operatius) i serveis informàtics, va endegar un grup de treball que s'havia d'encarregar de desenvolupar un sistema per controlar electrodomèstics i petits equips informàtics de la època, donant la possibilitat de que es connectessin en xarxa. El grup estava format per diversos enginyers, entre els que trobem Bill Joy, Andy Bechtolsheim, Wayne Rosing, Mike Sheridan, James Gosling i Patrick Naughton. El projecte duia per nom Green Project, i la idea era crear un hardware polivalent, un sistema operatiu eficient, i un llenguatge de programació relacionat. La seva idea era anticipar cap a on es dirigiria la computació en el futur, i es marquen com a objectiu el desenvolupament d'un entorn únic que pogués ser utilitzat per tots els dispositius d'electrònica de consum.

Il·lustració 31: Logo de Java

Amb aquesta idea, comencen a treballar al Febrer de 1991 a Sand Hill Road, a Menlo Park, California. Naughton com a encarregat del sistema gràfic, Gosling dedicat a identificar el llenguatge de programació més adient al projecte i Sheridan dedicat al desenvolupament de negoci.

Entre els objectius inicials de Gosling es trobava implementar una màquina virtual, i un llenguatge amb estructura i sintaxi similar a C++. Per aquest motiu, en un principi, es va pensar en C++ com a llenguatge de desenvolupament, estenent-lo i modificant-lo. Però la idea es va descartar, donant lloc a un nou llenguatge, que inicialment fou anomenat **Oak**, per un roure que hi havia fora de l'oficina de Gosling. .

L'anomenat Green Team va treballar gairebé dos anys en el projecte i a l'Agost de 1991 Oak ja executava els primers programes. També treballaven en un prototip anomenat Star7 (*7), similar a una PDA, que tenia aquest nom degut a la combinació de tecles del telèfon de la oficina del Green Project que permetia als usuaris respondre a les trucades des de qualsevol lloc.

Després de mostrar al CEO de Sun, Scott McNealy els prototips de baix nivell del sistema, el desenvolupament va continuar, amb el sistema operatiu GreenOS i el llenguatge de programació Oak. Al Setembre de 1992 finalitza el desenvolupament, i amb ell el Green Project.

Sun va crear una nova filial anomenada FirstPerson, encarregada de comercialitzar la nova tecnologia. Però aquest intent de comercialització no va ser l'èxit esperat. El mercat objectiu per al

qual es va crear *7, l'electrònica de consum, no va voler saber d'aquesta tecnologia, degut a l'excessiu preu i encariment dels productes final que generava, especialment en comparació amb altres solucions coetànies. Després de diversos intents de comercialització del producte a empreses de diferents camps, cap d'ells és favorable, i Sun desmantella FirstPerson, assumint el projecte com un fracàs.

D'entre tota la feina duta a terme pel Green Project, només va quedar el llenguatge de programació **Oak**. Amb l'aparició de la **World Wide Web**, i dels primers navegadors gràfics, com eren **Mosaic** o **ViolaWWW**, i veient l'elevat nombre de llocs webs que apareixien cada dia, Joy va decidir reorientar el projecte cap a la Web, ja que preveien que Internet es convertiria en un mitjà interactiu important en el futur. Per aquest motiu van començar a treballar en un navegador similar a Mosaic, anomenat inicialment WebRunner, en honor a la pel·lícula Blade Runner.

Donat que el nom Oak era ja una marca registrada per adaptadors de targetes gràfiques, es va haver de canviar el nom. En un principi, es va optar per **Green**, però finalment el nom triat fou **Java** (Il·lustració 31)**.** Existeixen diverses teories sobre l'origen d'aquest nom, i de si es tracta o no d'un acrònim. Hi ha qui diu que són les inicials dels seus creadors: ***J**ames Gosling, **A**rthur **V**an Hoff, i **A**ndy Bechtolsheim.* D'altres teories aposten per ***J**ust **A**nother **V**ague **A**cronym*, ("simplement un altre acrònim ambigu"). Però la teoria més estesa és que es tracta del nom d'un tipus de cafè que servien a una cafeteria propera a la seu de Sun, on es desenvolupava el projecte, i d'aquí la tassa de cafè fumejant del logotip de Java.

Al 29 de Setembre de 1994 es va finalitzar el desenvolupament del prototip WebRunner, conegut finalment amb el nom de HotJava. Aquest cop si, i després d'una demostració als alts executius de Sun Microsystems, es reconeix el gran potencial de Java, i el projecte es tira endavant.

Així, durant els inicis del 1995, es llençaren les primeres versions de Java. Al Maig d'aquell mateix any, en la conferència Sun World '95, es va anunciar una versió alpha, que funcionava únicament sobre Solaris, i que s'incorporaria al navegador més estès del moment, Netscape Navigator. Al Juliol del mateix any, amb la segona alpha, es va afegir suport per Windows NT, i amb la tercera, al mes d'Agost, per a Windows 95. Al 1996, Sun creava JavaSoft per desenvolupar la tecnologia, i durant el mateix mes apareix el primer kit de desenvolupament, el JDK (Java Development Kit) 1.0.

Gràcies a la decisió de Sun Microsystems de **distribuir de forma lliure** aquest llenguatge per la xarxa, concedint llicències a tothom que les volgués, es va aconseguir que molts desenvolupadors s'impliquessin en la depuració i millora del mateix. La seva difusió va ser vertiginosa a partir de llavors, i fou millorat amb multitud de noves classes i suport TCP/IP, convertint-lo en un dels llenguatges més difosos, i amb més especificacions i funcionalitats. Des de la JDK 1.0, Java ha experimentat nombrosos canvis, amb un gran increment en el nombre de classes que composen la biblioteca estàndard. A partir de la versió J2SE 1.4, el llenguatge ha estat regulat per la JCP (Java Community Process).

A l'any **2009 Sun Microsystems va ser adquirida per Oracle Corporation**, donant lloc a tota mena de rumors sobre la possibilitat de que tot el software lliure de la companyia responsable de Java, passes a ser privatiu. Sortosament, això no ha succeït per ara, i Java continua sent un llenguatge de programació de lliure distribució sota llicència de la GNU.

Definició

Java és un llenguatge de propòsit general apte per a crear tota mena d'aplicacions professionals. Molts fabricants l'han adoptat com la seva eina per al desenvolupament d'aplicacions comercials,

donat que els programes es poden executar en diversos equips. Això és una de les principals característiques de Java, que els programes es poden executar en múltiples equips diferents, independentment de l'arquitectura, el processador o el sistema operatiu.

Java és públic, qualsevol programador pot aconseguir un kit de desenvolupament(**JDK, Java Developer's Kit**) de forma gratuïta. Permet la creació, a més de programes més tradicionals, d'applets i servlets, que s'insereixen a les pàgines web i s'executen a l'ordinador local. Permet la creació de software interxarxes, client-servidor, distribuïdes per xarxa local o per Internet. A més és fiable i permet controlar l'accés als recursos del sistema, gestionar permisos i l'ús de criptografia, aportant seguretat.

Java és un llenguatge de programació que segueix el paradigma de **programació orientada a objectes** (**POO**), on s'empren objectes per al disseny de programes, i es basa en tècniques com:

- **L'encapsulament**: propietat que tenen els objectes d'ocultar els seus atributs i mètodes a altres parts del programa o altres objectes. La forma natural de construir una classe es definir uns atributs que no són accessibles des de fora del propi objecte, si no que únicament es poden modificar mitjançant els mètodes definits a tal efecte, i que són definits com a accessibles des de l'exterior.
- **L'herència**: propietat que permet definir classes descendents d'altres, de forma que la nova classe (la filla) hereta de la classe pare tots els seus atributs i mètodes. La nova classe pot definir nous atributs i mètodes i inclús redefinir els ja existents i heretats de la classe pare. Aquesta propietat permet la reutilització de codi, aprofitant el d'altres classes ja existents, i modificant-les mínimament per adaptar-les a les noves necessitats.
- **El polimorfisme**: propietat que permet que un mateix missatge enviat a objectes de classes diferents, faci que aquests es comportin de forma també diferent (objectes diferents poden tenir mètodes amb el mateix nom, i inclús un mateix objecte pot tenir noms de mètodes idèntics, però amb paràmetres diferents).

Els objectes són entitats que tenen un determinat estat, comportament i identitat:

- **Estat**: són les dades o informació que conte l'objecte, i que seran assignats amb uns valors concrets.
- **Comportament**: són els mètodes o missatges als que l'objecte sap respondre. És a dir, les operacions que l'objecte pot realitzar.
- **Identitat**: és la propietat de l'objecte que el diferencia de la resta. Es pot considerar com un identificador.

L'objecte conté tota la informació que permet diferenciar-lo de la resta d'objectes, tant de la mateixa classe, com d'altres. Els objectes disposen de mètodes per a la seva interacció, i que permeten el canvi del seu estat. En el paradigma de programació orientada a objectes, **mètodes** i **atributs** tenen una estreta relació, donat que **la modificació dels atributs sempre es realitza a través de mètodes** (**getters** i **setters**). Aquesta és una gran diferència respecte a la programació estructurada tradicional, on a partir d'una sèrie de dades, s'esperen unes dades de sortida, i per aconseguir-ho, primer es pensen les funcions que duran a terme el procés, i després, quines seran les

estructures de dades necessàries per a l'emmagatzemament, i que seran processades. En la POO, únicament es definiran objectes, i després se'ls enviaran missatges sol·licitant que realitzin els mètodes per si mateixos. Cal **diferenciar** entre **objecte** i **classe**. Anàlogament a com es declaren les variables en qualsevol llenguatge de programació, on s'assigna un nom a la variable, i es defineix el tipus de variable a que pertany, en llenguatges orientats a objectes, els **objectes es declaren definint a quin tipus de classe pertanyen**. D'aquesta forma, un objecte A pertanyent a la classe CLASS, tindrà tots els atributs i mètodes que formen la classe CLASS. Direm que A és una instància de CLASS.

Java és un llenguatge fàcil d'aprendre, i no permet al programador abandonar la POO, evitant el retorn a tipus de sistemes de programació tradicionals. A mesura que el programador es va adaptant es fomenten bons estils de programació, i finalment, gràcies a les avantatges que dóna la POO, pocs programadors no el consideren el seu llenguatge favorit.

Java té les següents característiques:

- És intrínsecament orientat a objectes.
- Funciona perfectament en xarxa.
- Té una gran funcionalitat, gràcies a les seves llibreries de classes.
- El programador no pot fer servir punters, ja que el propi llenguatge els fa servir de forma transparent.
- El propi llenguatge es fa càrrec de la gestió de memòria, i no el programador, convertint Java en un llenguatge robust i susceptible de tenir pocs errors per aquest motiu.
- Les aplicacions finals tenen poc marge d'error possible.
- Incorpora Multi-Threading(tasques concurrents dins un mateix programa).

Tot i que **Java** es pot considerar una evolució de C++, **va ser escrit partint de zero**, permetent que el resultat final sigui un llenguatge purament orientat a objectes, i que no permet programar mitjançant altres tècniques o paradigmes. Tot i que estrictament parlant és un llenguatge interpretat, necessita d'una "compilació" prèvia, que genera un fitxer que emmagatzema el "**bytecode**", o "**j_code**", un pseudocodi gairebé igual al codi màquina. Per a la seva execució, caldrà un interpret, l'anomenada **Màquina Virtual de Java (JVM, Java Virtual Machine**). Aquesta JVM és la idea revolucionaria que va introduir Java, i que permet independència respecte a l'equip en que s'està executant. Dóna igual en quina màquina sigui "compilat" el programa Java, ja que el bytecode final generat serà el mateix, escrit en un llenguatge només interpretable per una màquina en forma virtual. La JVM de cada equip serà diferent, adaptada a l'equip on s'instal·la, i serà aquesta l'encarregada de fer la traducció al processador de l'equip on s'executa el programa. Donat que aquesta interpretació es fa pràcticament a nivell de codi màquina, no hi ha greus pèrdues d'eficiència en quant a velocitat.

Per iniciar-se en el desenvolupament d'aplicacions Java, és necessari disposar del JDK (Java Developer's Kit), que és, bàsicament, un compilador i un intèrpret (Java Virtual Machine) per a línia de comandes. Existeixen nombrosos IDE's (Integrated Development Environment) per a la programació en Java. Entre els més coneguts trobem NetBeans, Eclipse, JCreator, BlueJ o JBuilder.

En el nostre cas hem treballat amb la versió de Java JRE 1.7.0_07 i l'OpenJDK 6. L'IDE que hem emprat és Spring Source ToolSuite, versió 2.9.0, una modificació de l'entorn de desenvolupament Eclipse.

4.2.2 Spring

Spring Framework

Il·lustració 32: Logotip d'Spring

Introducció

Als inicis de les tecnologies J2EE, EJB_1 el desenvolupament d'aplicacions era molt complexe i feixuc, repercutint inevitablement, en aplicacions més costoses. Per aquest motiu, Rod Johnson, programador de J2EE , va escriure la primera versió d'**Spring Framework** (Il·lustració 32) llançada al juny de 2003 sota la llicència d'Apache 2.0 i juntament amb el seu llibre *Expert One-on-One J2EE Design an Development* (Wrox Press, octubre 2002).

Encara que la primera versió d'Spring fou llençada al 2003, el gran llançament es produiria un any més tard, en concret, al Març de 2004 amb la versió Spring 1.0. Posteriorment, més actualitzacions foren llençades al setembre de 2004, març de 2005, març de 2006, aquesta última obtingué premis com els Jolt Awards i Jax Innovation Awards. Spring Framework 2.0 fou llençada l'any 2006, la versió 2.5 l'any 2007, la versió 3.0 l'any 2009, la versió 3.1 l'any 2011. Actualment Spring Framework es troba a la versió 3.2.3

Definició

Spring és un framework de codi obert que permet el desenvolupament d'aplicacions utilitzant el llenguatge Java. El nucli d'Spring està basat en un principi o patró de disseny anomenat Inversió de Control (IoC, Inversion of Control) i aquest és un dels motius principals pels quals Spring està tan acceptat dins els frameworks de desenvolupament d'aplicacions. L'utilització de llenguatge Java, implica la programació orientada a aspectes (POA). És considerat com una alternativa, complement, o inclús substitut del model EJB_1 (Enterprise JavaBean). Per tot això, i pel seu mòdul MVC, que gaudeix d'una gran popularitat, Spring és considerat un dels frameworks de codi lliure més importants en l'actualitat.

Segons el manual de referència, *"Spring Framework is a Java platform that provides comprehensive infrastructure support for developing Java applications. Spring handles the infrastructure so you can focus on your application."* La seva traducció literal és, **Spring Framework és una plataforma que ens proporciona una infraestructura que actua de suport per desenvolupar aplicacions Java. Spring s'encarrega de la infraestructura, i tu et pots**

centrar en la teva aplicació. Spring s'encarrega de tota la infraestructura, és a dir, uneix tots els components de l'aplicació i controla la interacció entre ells, els seus cicles de vida, etc...D'aquesta manera el programador únicament s'ha de preocupar de desenvolupar l'aplicació en si.

Spring Framewok s'utilitza per a desenvolupar aplicacions web, encara que segons la seva definició, permet desenvolupar qualsevol tipus d'aplicació Java. S'utilitza principalment en entorns web gràcies a que és un contenidor lleuger en contraposició a un servidor d'aplicacions J2EE. És suficient un contenidor de servlets com Tomcat per poder executar tota l'aplicació.

Injecció de dependències

La injecció de dependències és un patró de disseny orientat a objectes en que un objecte interactua amb altres objectes amb la particularitat que no es l'objecte qui crea els objectes que necessita, si no que aquests són subministrats a l'objecte que els requereix. L'objectiu és aconseguir un baix acoblament entre els objectes de l'aplicació. Aquesta interacció pot ser la invocació de mètodes o l'obtenció d'atributs dels objectes.

Sense aplicar aquest patró, l'objecte seria l'encarregat d'instanciar (directament amb el seu constructor) o localitzar les dependències (objectes) amb les que treballa (utilitzant un localitzador de serveis). Aplicant aquest patró (DI, Dependency Injection), l'objecte solament defineix els objectes amb que interactuarà i serà un contenidor qui injectarà aquests objectes al crear el Bean (IoC).

L'objecte pot definir els objectes amb que interactuarà de 3 maneres diferents:

- A través dels arguments del seu constructor.
- Amb arguments a un mètode de factory.
- A través de mètodes setters invocats després de la construcció dels objectes.

La forma habitual d'aplicar aquest patró és mitjançant un “Contenedor DI” i objectes plans o simples com els POJO de Java. El contenidor injecta a cada objecte, segons estiguin definits en un fitxer de configuració XML, altres objectes necessaris i les seves relacions.

Podem veure l'aplicació d'aquest patró amb el següent exemple on tenim una classe A que interactua amb una classe B. Primer sense aplicar DI on s'observa l'alt acoblament d'A amb B:

Sense aplicar DI:

```
public class A{
  private B b;

  public A{
    b = new B();
  }

  public void realitzarAccioA(){
        b.realitzarAccioB();
  }
}


public class B{
```

```
  public B{
  }

  public void realitzarAccioB(){
        System.out.println("S'esta executant el mètode realitzarAccioB de la classe B);
  }
}
```

Com es pot observar existeix un acoblament d'A amb B i és la classe A que s'encarrega d'instanciar la classe B i cridar al mètode que desitja. Si apliquem el patró DI a continuació observem el baix acoblament entre A i B. A ja no té la necessitat d'instanciar B. En aquest cas s'escull definir B a A a través del constructor.

Aplicant DI:

```
public class B{

  public B{
  }

  public void realitzarAccioB(){
        System.out.println("S'esta executant el mètode realitzarAccioB de la classe B);
  }
}

public class A{
  private B b;

  public A(B bb){
    b = bb;
  }

  public void realitzarAccioA(){
        b.realitzarAccioB();
  }
}
```

Inversió de Control (IoC)

Per tal de poder aplicar el patró injecció de dependència necessitem un "Contenidor DI" i objectes plans o simples com els POJO de Java. El contenidor injecta a cada objecte altres objectes necessaris. Doncs bé, aquest contenidor és implementat a través d'Spring i posteriorment serà qui injecti els objectes a l'objecte que els necessiti. L'objecte no caldrà que apliqui la injecció de dependència a través del seu constructor, setters, etc... si no que seran injectats dins ell a través d'aquest contenidor. Aquest és el principi d'inversió de control IoC, ja que no és la classe qui demana les dependències si no que aquestes són donades a la classe. Aquest motiu fa que es pugui associar al "principi de Hollywood": "No ens truqui, nosaltres el trucarem". El codi de l'usuari no invoca a un mètode d'una biblioteca si no que és la biblioteca qui invoca el codi de l'usuari.

La IoC es definiria com un contenidor que ens facilita aplicar el patró DI i no ser nosaltres qui ho fem, com a l'exemple de l'apartat anterior. Nosaltres diem al contenidor la implementació concreta de les classes per a les dependències, ell (el contenidor) instancia els objectes i assegura que els constructors i setters siguin executats amb els objectes correctes.

Spring facilita, entre altres, el contenidor de DI Application Context, que no és res més que un

fitxer de configuració IoC en XML. Dins d'aquest fitxer els POJO són anomenats BEANS (els objectes amb les seves dependències definides) si el contenidor DI l'implementa el Framework Spring, com és el cas.

A continuació podem veure un exemple que realitza DI amb IoC a través del contenidor d'Spring Application Context, beneficiant l'aplicació amb tot l'esmentat anteriorment, i, a més, amb la reducció del codi de les aplicacions, l'externalització de les dependències. Aquestes es gestionen des d'un sol lloc i fa que les provatures siguin fàcils:

```
public interface cama{
   void xutaPenal();
}

public class dreta implements cama{
   @Override
   public void xuta(){
      System.out.println(“Goool!!! Sóc dretà);
   }
}

public class esquerra implements cama{
   @Override
   public void xuta(){
      System.out.println(“Ohhh!!! He fallat. Sóc dretà”);
   }
}

public class Futbolista{
  private Cama cama;

  public void xutaPenal(){
    System.out.println(“Xutant el penal i.....”);
    cama.xuta();
  }

  public void setCama(Cama cama){
    this.cama = cama;
  }
  public Cama getCama(){
     return cama;
  }
}

public static void main(String[] args){
  ApplicationContext applicationContext=new ClassPatchXmlApplicationContext(“application-context.xml”);
  Futbolista futbolista = (Futbolista)applicationContext.getBean(“futbolistaEsquerrà”);
  futbolista.xutaPenal();
}
```

Fitxer de configuració aplication-context.xml:

```
<class="xml" name="code"><beans xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="http://www.springframework.org/schema/beans"
xsi:schemalocation="http://www.springframework.org/schema/beans
http://www.springframework.org/schema/beans/spring-beans-3.0.xsd">
```

```
<bean class="com.sample.Dreta" id="dreta"></bean>
<bean class="com.sample.Esquerra" id="esquerra"></bean>

<bean class="com.sample.Futbolista" id="futbolistaEsquerrà">
<property name="cama" ref="esquerra"></property>
</bean>
</beans>
```

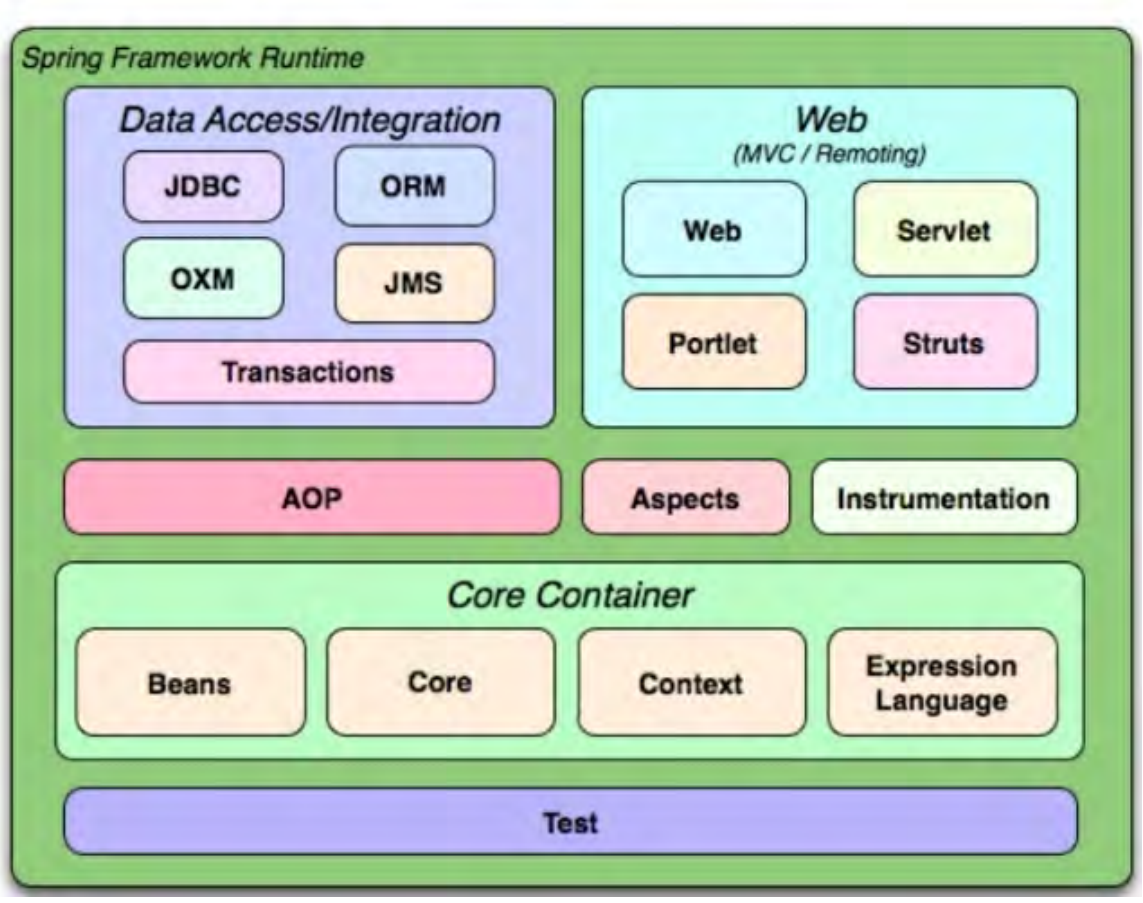
El programa escriurà a la línia de comandes: Ohhh!!! He fallat. Sóc dretà.

Mòduls i característiques

Tot el **Framework Spring** es troba organitzat amb uns **20 mòduls** que inclouen tot el que Spring pot oferir (Il·lustració 33). En un projecte no tots els mòduls d'Spring ha de ser utilitzats, únicament els que nosaltres necessitem. A més, gràcies a la pròpia estructura modular del Framework, podem intercanviar mòduls que té Spring per d'altres Frameworks que realitzin les mateixes funcions.

Per exemple, si es realitza una aplicació web, utilitzarem el mòdul Spring MVC, però no és obligatori. Podem utilitzar qualsevol altre Framework web, com per exemple Struts.

Com que s'utilitzen els mòduls que es desitgen, aquests no es troben inclosos a l'aplicació s'han d'importar segons les necessitats. A més existeixen algunes dependències entre mòduls. Per no haver d'estar pendent d'aquests aspectes, s'utilitza Maven, que pot obtenir totes les llibreries necessàries i resoldre aquestes dependències de forma automàtica.



Il·lustració 33: Mòduls d'Spring

Com es pot observar les mòduls estan agrupats amb les capes “Core Container”, “Data Access/Integration”, “Web”, “AOP”, “Instrumentation” i “Test”.

Capa Core Container:

Contenidor d'Inversió de Control. Permet la configuració dels components de l'aplicació i l'administració del cicle de vida dels objectes Java. Es duu a terme principalment a través de la injecció de dependències.
Els mòduls Core i Beans aporten les parts fonamentals del Framework, incloent IoC i la injecció de dependències. Bean Factory és una sofisticada implementació del patró Factory. Aquesta elimina la necessitat d'implementar Singletons i permet desacoplar la configuració de l'especificació de dependències del model lògic.
El mòdul Context es construeix a partir de la sòlida base que proporcionen Core i Beans. Aquest mòdul hereta característiques de Beans, afegeix suport per la internacionalització, propagació d'events i creació transparent de contextos, com per exemple el Servlet container. Solament té suport per característiques de JEE com EJB i JMX. Aquí és on s'inclou la interfície AplicationContext que és un fitxer de configuració bàsica d'Spring en xml.
Expression Language proporciona un fort llenguatge d'expressions per manipular objectes en temps d'execució. És una extensió del Llenguatge d'Expressions unificat especificat a les especificacions de JSP 2.1. El llenguatge suporta mètodes getters i setters, assignació de propietats, crida de mètodes, accés a arrays de contexts, col·leccions, índexs, operadors lògics i aritmètics i creació de variables del contenidor IoC de Spring.

Capa Data Access/Integration:

- JDBC proporciona una abstracció del model JDBC i elimina la necessitat d'utilitzar el JDBC bàsic que proporciona JAVA per accedir a la BD i controlar els errors.
- ORM proporciona una capa d'integració per les API's de mapatge entre objectes i el model relacional. Inclou integració amb Hibernate, JPA, JDO i iBatis. Aquest mòdul permet integrar els Frameworks anteriors amb la funcionalitat i característiques que ofereix Spring.
- OXM proporciona una capa d'abstracció que suporta el mapatge Object/XML implementat per JAXB, Castor, XMLBeans, JiBX i Xstream.
- JSM proporciona característiques per enviar i rebre missatges.
- Transaction proporciona suport per transaccions de gestió de transaccions programàtiques i declaratives per a les classes que implementen les interfícies especials i per tots els seus POJOs.

Capa Web:

Web facilita un model bàsic orientat a la integració i la inicialització del contenidor IoC utilitzant “servlet containers” i context d'aplicació orientat a la web.
Servlet conté la implementació del model MVC d'Spring per aplicacions web.
Struts proporciona la integració del Framework Struts.
Portlet proporciona la implementació MVC per desenvolupar portlets.

Capa aop:

Proporciona la implementació per definir el model de programació orientada a aspectes.

Capa instrumentation:

Proporciona ajuda instrumental a la classe i a les implementacions del carregador de classe per a que pugui ser utilitzat a aplicacions servlet.

Capa test:

Proporciona el testeig dels components d'Spring amb JUnit o TestNG.

Els mòduls anteriors donen a Spring les seves característiques principals (versió 2.5):

- Simplificació de la programació orientada a aspectes.
- Simplificació de l'accés a dades.
- Simplificació i integració amb JEE.
- Suport per la planificació de treballs.
- Suport per l'enviament de correus electrònics.
- Interacció amb llenguatges dinàmics. (BeanShell, JRuby, Groovy)
- Suport per accés a components remots.
- Maneig de Transaccions.
- El seu propi Framework MVC.
- El seu propi Web Flow.
- Maneig simplificat d'excepcions.

La versió Spring 3.0 afegeix a les característiques anteriors les següents entre d'altres:

- Suport per a Java 5: Proporciona configuració basada en anotacions i suporta característiques com varargs i genèrics. A més, la part web és compatible amb les versions 1.4 i 5 de JEE implicant així tenir necessàriament la versió JRE 5 o superior.
- Llenguatge d'Expressions (SpEL): S'inclou un llenguatge d'expressions que pot ser utilitzat al definir les Beans, tant en XML com amb anotacions i també dóna suport a través de tots els mòduls Spring.
- Suport per Serveis Web REST.
- Suport per Java EE6: Ofereix suport de característiques com JPS 2.0, JSF2.0 i JRS 303(validació de Beans).
- Suport de BD encastades: Ofereix suport per a HSQL, H2 i Derby.
- Suport per la formatació de dates mitjançant anotacions: Els camps de dates, monedes, etc.. seran formatades i transformats automàticament utilitzant anotacions.
- Nova organització dels mòduls: Els mòduls han estat revisats i separats i els paquets nous són:
    - org.springframework.aop
    - org.springframework.beans
    - org.springframework.context
    - org.springframework.context.support
    - org.springframework.expression
    - org.springframework.instrument
    - org.springframework.jdbc

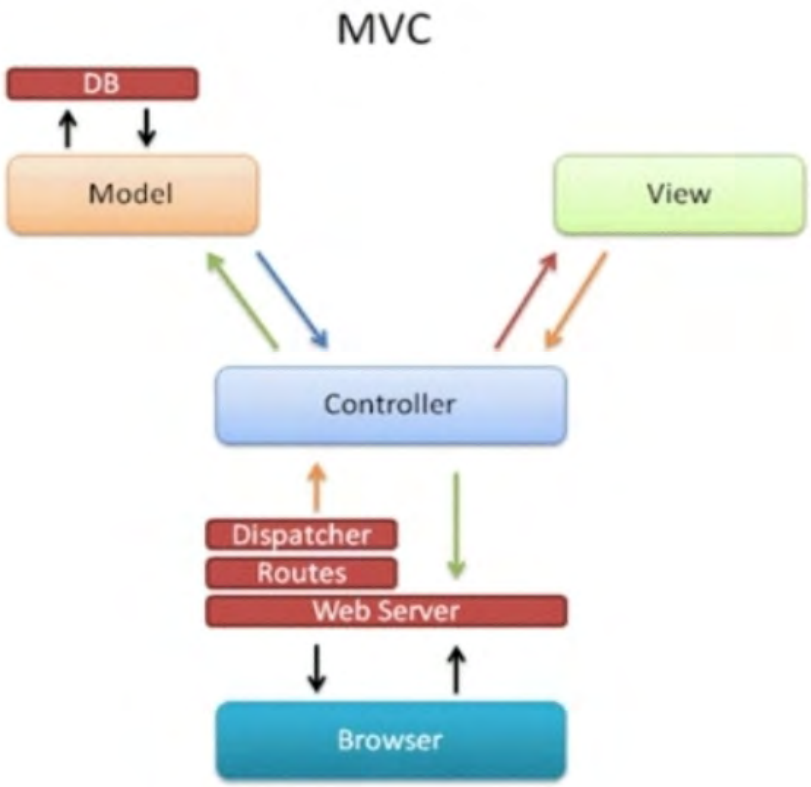
- org.springframework.jms
- org.springframework.orm
- org.springframework.oxm
- org.springframework.test
- org.springframework.transaction
- org.springframework.web
- org.springframework.web.portlet
- org.springframework.web.servlet
- org.springframework.web.struts

Spring MVC

És un dels principals mòduls del Framework Spring, i un dels més utilitzats, a més de ser el responsable de la gran acceptació que disposa aquest Framework. Implementa el MVC i forma part del paquet web. No és obligatori utilitzar aquest mòdul per poder crear una aplicació web basada amb Spring ja que podem utilitzar d'altres Frameworks MVC com Struts. No obstant, proveeix un exhaustiu suport pel patró MVC i proveeix altres característiques com facilitar la implementació de la capa presentació.

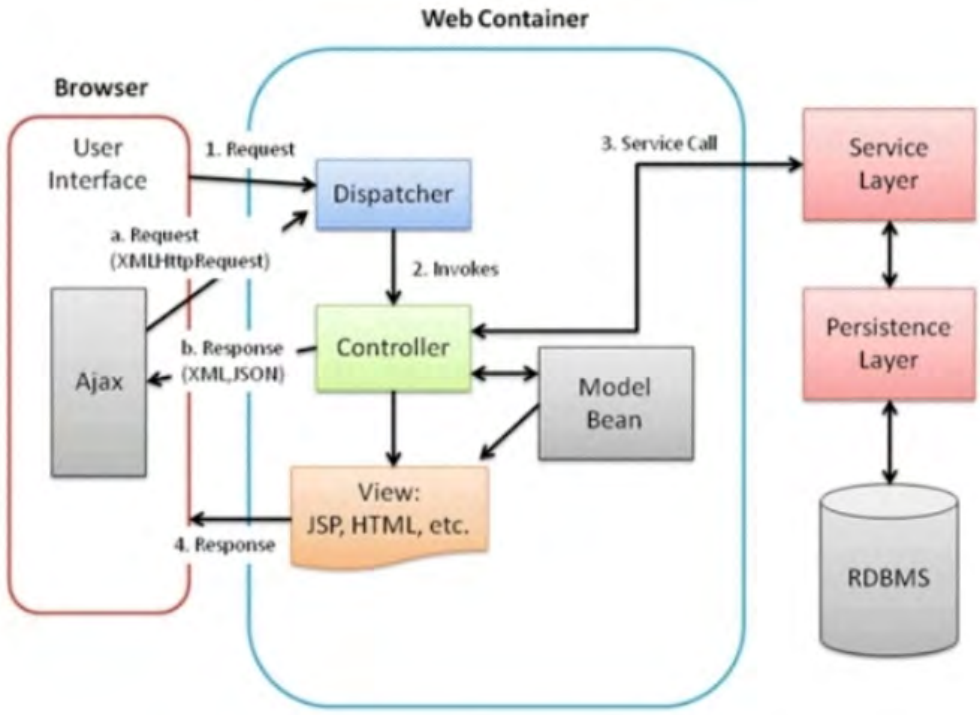
Aquest MVC és el patró de software que separa l'aplicació en tres capes (Il·lustració 34):

- Model: representa les dades o regles de negoci i l'estat de l'aplicació.
- Vista: representació les dades a l'usuari de forma específica, la interfície d'usuari.
- Controlador: gestiona les sol·licituds de les accions realitzades de l'usuari a la vista, actualitza el model i redirigeix els resultats de l'execució de les dades a la vista per l'usuari, és a dir, la capa de negoci.



Il·lustració 34: Visió de conjunt del model Vista Controlador

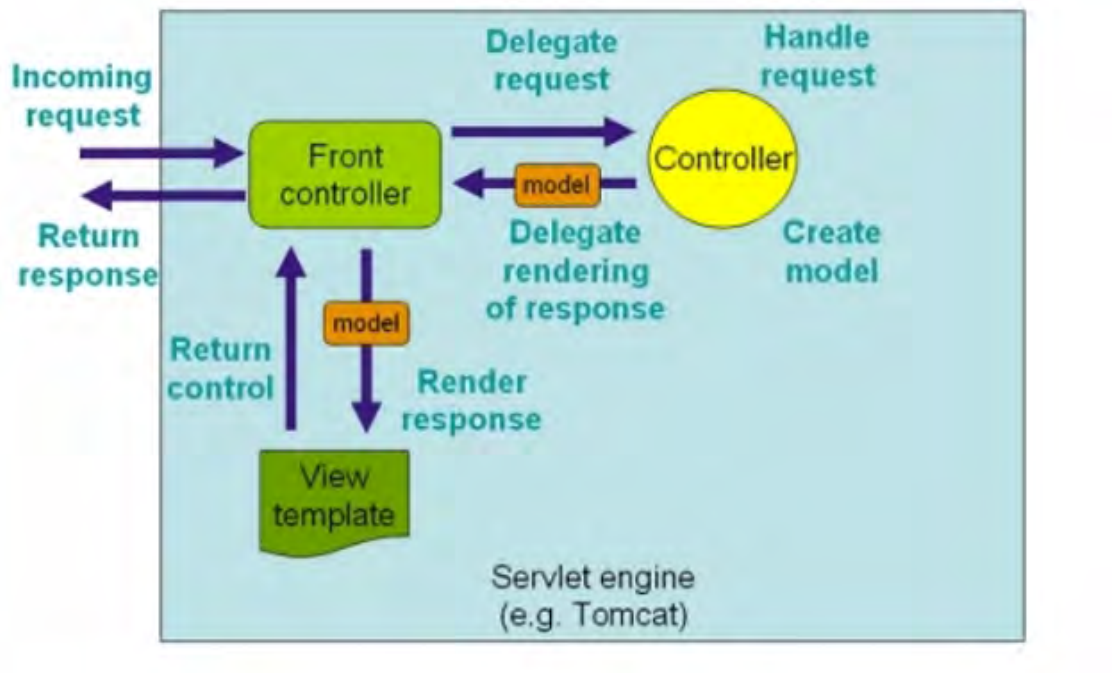
Aquest MVC ha anat evolucionat adoptant llenguatges com AJAX, Javascript, JSON o XML adoptant l'esquema actualitzat següent(Il·lustració 35):



Il·lustració 35: Model Vista controlador amb AJAX

Spring MVC adopta aquesta estructura de capes o nivells i gestiona el patró tal com es mostra a la següent il·lustració. Està dissenyat al voltant d'un servlet central que distribueix les sol·licituds als controladors. Aquest servlet s'anomena DispatcherServlet i aplica el patró Front Controller, està integrat dins el IoC d'Spring adoptant així totes les seves característiques.

El cicle d'una petició amb Spring 3.0 MVC és el següent (Il·lustració 36):



Il·lustració 36: Cicle de vida d'una petició a Spring MVC

1- S'envia una petició web HTTP al contenidor web.

2- Aquesta petició la intercepta el Front Controller i obté el Handler Mapping.

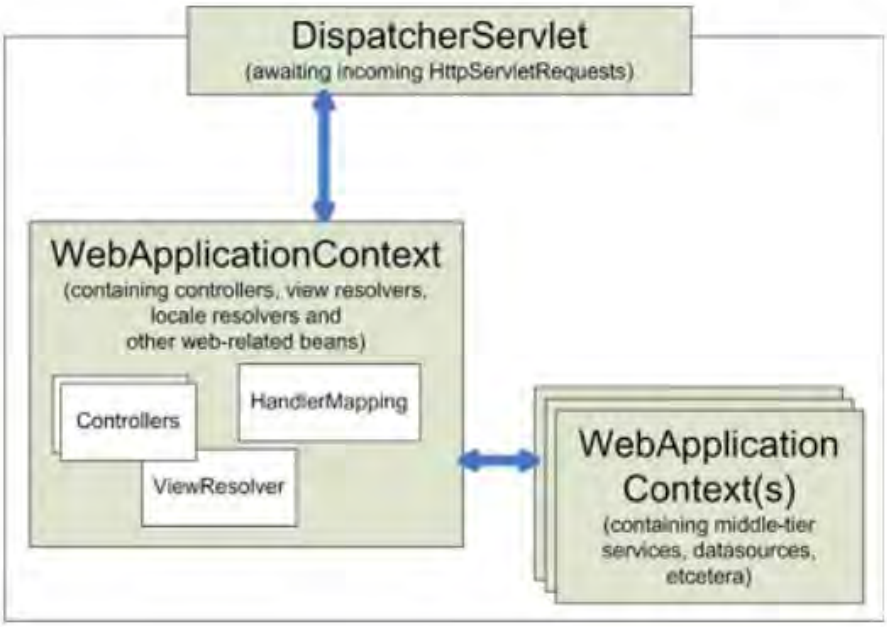
3- El DispacherServlet, amb l'ajuda dels Handler Mappings envia la petició al controlador oportú.

4- El controlador processa la petició i retorna l'objecte Model and View amb la vista i objectes del model.

5- El Front Controller resol la vista (JSP, Velocity, Tiles, etc...)

6- La vista creada s'envia al client.

Com es pot observar, el **DispatcherServlet** és l'element més important d'aquest model MVC (Il·lustració 37).



Il·lustració 37: Arquitectura d'Spring

Spring Security

Introducció

A finals de 2003 s'inicia un projecte anomenat **Acegi Security** per dotar de seguretat a aplicacions. Al Març de 2004 apareix la primera versió d'aquest sota llicència Apache License. Al Maig del 2006 es llença ja Acegi Security 1.0.0. Durant els següents dos anys i mig, és utilitzat en multitud de projectes software fins que és adoptat per Spring passant-ne a formar part com un subprojecte seu anomenat **Spring Security**.

La primera versió Spring Security comença amb la 2.0 i després es llença la 3.0. Aquest està basat amb les sòlides bases adoptades del seu predecessor Acegi Security.

Definició

Spring Security és un dels **Framework de seguretat més populars i complerts** sobre aplicacions basades en arquitectura J2EE. Spring Security aporta tota la infraestructura de seguretat per aplicacions realitzades sobre el Framework Spring i està basat sobre aquest. És una plataforma de codi obert i en constant evolució, cosa que implica l'adopció de nous mecanismes d'autenticació per tal d'adaptar-se, o bé dóna la possibilitat de desenvolupar-los un mateix de manera fàcil.

Característiques

Spring Security està basat íntegrament en el Framework Spring, adopta d'aquest molts conceptes com la injecció de dependències, inversió de control i la programació orientada a aspectes. Això fa que la integració amb una aplicació basada amb Spring sigui total i els coneixements d'aquest facilitin enormement el desenvolupament amb Spring Security.

Una de les millors característiques és que no és invasiu, no t'obliga a modificar el codi de l'aplicació o tenir en compte l'ús del Framework als inicis. Això no vol dir que no s'hagi de desenvolupar codi, com algun proveïdor d'autenticació per validar usuari i contrasenya, però gràcies al principi de disseny “programar cap a interfícies, no implementacions” i al DI container d'Spring no s'ha de modificar el codi existent. Corrobora, doncs, un altre principi, “tancat per modificació, obert per extensió”.

Aquestes particularitats, juntament amb altres, fan que el Framework proporcioni les característiques següents:

- Fàcil configuració utilitzant la injecció de dependències d'Spring.
- Desplegament de l'aplicació no intrusiu.
- Codi no invasiu.
- Arquitectura escalable.
- Serveis integrals d'autorització.
  - Sintaxi basada en expressió de llenguatges.
  - Autorització de peticions HTTP.
  - Seguretat a la capa serveis.
    - Anotacions de seguretat JSR-250 ("EJB 3")
    - Anotacions d'invocació @Pre and @Post
    - Suport d'AspectJ
  - Seguretat a instàncies d'objectes del domini.
- Integra CAS 3.
- Suporta OpenID.
- Suporta certificats X.509.
- Suporta LDAP.
- APIs d'aprovisionament.
- Suporta autenticació HTTP BASIC.
- Suporta autenticació HTTP Digest.
- Diversos backends d'autenticació.
- Fàcil integració amb bases de dades existents.
- Codificació de contrasenyes.

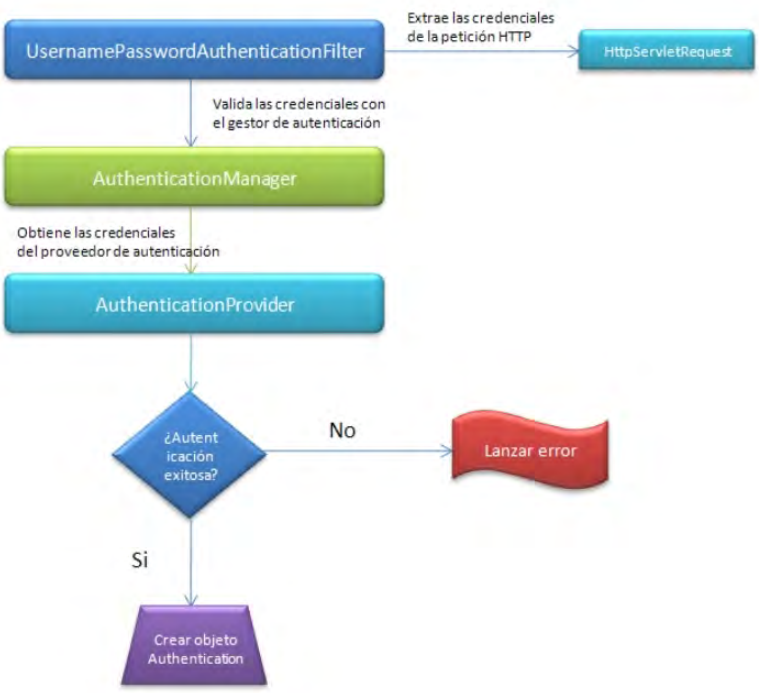
- Caching.
- Suport d'events.
- Suport remot.
- Propagació de la seguretat entre ordinadors client.
- Run-as reposició de la persona autenticada.
- Compatibilitat amb Servlet Security API.
- Seguretat del canal HTTPS.
- Suporta tag library.
- Flexible amb la integració de Frameworks addicionals d'autenticació.
- Autenticació persistent utilitzant el recorda'm.
- Suport d'IDE.
- Suporta Spring Web Flow.
- Facilitat de peer review.
- Suport comercial.
- Llicència Apache.

Un cop vistes les característiques, Spring Security gestiona dos aspectes fonamentals de seguretat: l'autorització i l'autenticació. És obvi que l'autorització depèn de l'autenticació perquè aquesta última es produeix primer.

– **Autenticació** (Il·lustració 38): Amb l'autenticació s'aconsegueix saber que l'usuari de l'aplicació és qui diu ser. Aquest usuari se l'anomena “principal”. Per realitzar aquest procés Spring Security ofereix un gran nombre de mecanismes, inclús podem crear el nostre propi proveïdor d'autenticació. Les dades que aquest últim necessita per poder autenticar els usuaris correctament es poden guardar a memòria, a bases de dades relacionals (es pot configurar per a que guardi les dades encriptades), repositoris LDAP, sistemes OpenID, etc... Es poden canviar els tipus d'autenticació sense tocar el codi.

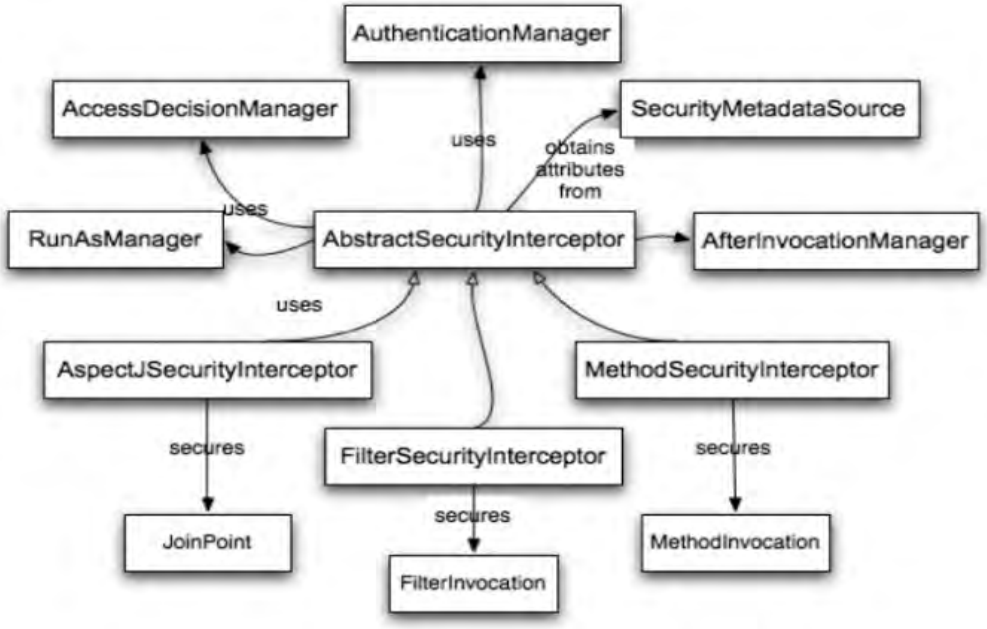
Com ja s'ha vist, el Framework ofereix múltiples opcions per l'autenticació però totes necessiten el component AuthenticationManager, principal component, a més d'altres components centrals:

- **SecurityContextHolder:** Emmagatzema les dades del “principal” i els seus rols.
- **Authentication:** Representació del “principal” amb els seus rols. És un objecte que es guarda dins el SecurityContextHolder.
- **UserDetailsService:** S'encarrega d'obtenir la informació de l'usuari que és vol autenticar de la font on estiguin emmagatzemades



Il·lustració 38: Procés d'autenticació d'Spring Security

– **Autorització**: el procés d'autorització és independent del d'autenticació i els components implicats es detallen a continuació. El principal component del procés d'autorització és l'**AbstractSecurityInterceptor** (Il·lustració 39), que facilita a funcionalitat bàsica de l'autorització. Els objectes per autoritzar són peticions HTTP a través de FilterSecurityInterceptor i invocacions a mètodes mitjançant MethodSecurityInterceptor i AspectJSecurityInterceptor. L'AbstractSecurityInterceptor delega l'autorització final a AccessDecisionManager. Aquest implementa un mètode anomenat "decide" que rep un objecte Authentication, un recurs segur (URL o execució d'un mètode) i una llista d'autoritats. Amb aquest paràmetres es decideix l'accés o no.



Il·lustració 39: Security Interceptor

4.2.3 MySQL

Il·lustració 40: Logo de MySQL

Introducció

En els sistemes informàtics, sempre ha estat necessari l'emmagatzemament de les dades amb les que es treballa. Per aquest motiu, des dels orígens de la computació van sorgir els sistemes gestors de bases de dades, conjunts de programes dedicats a l'emmagatzemament, recuperació, modificació i anàlisi de les dades.

Segons va passar el temps, es van començar a proveir mètodes per garantir la integritat de les dades, sistemes d'administració de l'accés d'usuaris, sistemes de recuperació d'informació en cas d'errors i moltes altres característiques i accessoris, com generadors d'informes o interfícies gràfiques per a la manipulació de la base de dades.

Hi va haver diverses aproximacions als anys 60 sobre l'estructura que havien de tenir les bases de dades en els sistemes de computació, com les bases de dades d'estructura jeràrquica, o les d'estructura de xarxa. Però Edgar Codd, treballador de IBM descontent amb la manca de funcions de cerca, va introduir als 70 el concepte de les bases de dades relacionals, culminant amb el document “A Relational Model of Data for Large Shared Data Banks”. En aquest article, Codd va introduir un nou sistema per a l'emmagatzemament i processament de les dades. Aquestes ja no s'emmagatzemaven en una llista encadenada de diferents registres de tipus de dades arbitraris, on molts dels camps podien quedar en blanc en el cas que aquestes dades no fossin necessàries,com en el primitiu sistema CODASYL. Amb el model relacional, la informació s'emmagatzema en una sèrie de taules que contenen registres. Les taules es relacionen entre sí de forma ordenada i normalitzada mitjançant uns camps clau, de tal forma que elements optatius són eliminats de la taula principal, evitant la creació de camps en blanc innecessaris. Per exemple, si es necessita emmagatzemar informació personal sobre els treballadors d'una empresa, en els models anteriors, un usuari del que no es disposa del número de telèfon generaria un camp en blanc al lloc on hauria de trobar-se aquesta informació. Amb les bases de dades relacionals, les dades sobre el número de

telèfon se separarien en una altra taula, i si no es disposa d'aquesta informació, simplement no es crearien registres relacionats amb la taula principal de treballadors.

En aquests sistemes gestors de bases de dades, el disseny previ és clau per al seu bon funcionament i coherència. S'ha de separar de forma correcta la informació que anirà en cadascuna de les taules segons les necessitats, quines d'aquestes dades seran les que identificaran de forma inequívoca cada element emmagatzemat i quines seran les relacions que existiran entre cadascuna de les taules.

Per al maneig d'aquesta informació, Codd va pensar en un llenguatge orientat a conjunts, que finalment va derivar en el llenguatge SQL, basat en una branca de l'àlgebra anomenada càlcul de tuples, ja que va demostrar que amb ella es podien dur a terme les operacions més típiques d'una base de dades, a més d'extreure conjunts de dades fàcilment.

L'article de Codd va inspirar diverses aproximacions a aquesta nova forma de creació de sistemes gestors de bases de dades. Basant-se llunyanament en les seves idees, IBM va començar a desenvolupar el seu propi sistema, anomenat System R, i fent servir com a llenguatge d'accés a les dades l'anomenat SEQUEL, el precursor del SQL que es va convertir en estàndard. D'altra banda, l'article de Codd va arribar a Eugene Wong i Michael StoneBraker, dos científics de Berkeley van iniciar el projecte INGRES, amb els fons destinats a la creació d'una base de dades geogràfica feta pel seus estudiants, i generant les primeres versions a l'any 79. El resultat va ser molt similar a al treball realitzat per IBM, incloent-hi el llenguatge d'accés, QUEL, tot i que finalment es va prendre SQL com a estàndard.

Moltes empreses van crear les seves solucions comercials per a implementar sistemes gestors de bases de dades des d'aquest moment. Entre les primeres trobem Sybase, Informix, NonStopSQL, MimerSQL i la pròpia INGRES. Només Larry Ellison, fundador d'Oracle, va iniciar un camí diferent basant-se en un article de IBM sobre System R. Amb el pas del temps, han aparegut moltes altres solucions, i s'han anat perfeccionant les originals. Entre els més emprats avui dia trobem DB2, Informix, Interbase, Microsoft SQL Server, Oracle, PostgreSQL, Firebird, SQLite i un llarg etcètera. Però el sistema triat per a la nostra aplicació ha estat MySQL (Il·lustració 40).

Definició

MySQL és un sistema gestor de bases de dades relacional, multifil i multiusuari, que des de l'any 2008 és propietat de Sun Microsystems. L'any 2009, amb l'adquisició de Sun per part de Oracle, MySQL va passar a ser propietat, per tant, del gegant mundial del software Oracle. MySQL funciona mitjançant un sistema de llicència dual. Habitualment s'ofereix sota la GNU GPL per a usos compatibles amb aquesta llicència. Però en el cas que alguna empresa el vulgui fer servir incorporant-lo en productes privatius, s'han de fer amb una llicència específica que els permeti el seu ús.

Aquest sistema de llicències duals, amb una part de caire privatiu, es pot realitzar d'aquesta forma, degut a que MySQL no és un software desenvolupat per la comunitat pública, i amb els drets d'autor en poder d'un autor individual, si no que una empresa privada el patrocina i n'és la propietària dels drets de la major part del codi.

MySQL disposa de diverses interfícies de programació en múltiples llenguatges, des de C fins a PHP, passant per Ruby, Pascal o Python. També existeix una interfície ODBC (Open DataBase Connectivity) anomenat MyODBC, i és accessible des de la ERP SAP.

MySQL és una base de dades molt ràpida en la lectura quan s'utilitza el motor no transaccional MyISAM, però en entorns d'elevada concurrència per a la modificació de dades, pot generar problemes d'integritat. És un sistema ideal en entorns d'alta concurrència per a lectura, però baixa per a modificació. És recomanable la monitorització del rendiment, per la correcció d'errors, tant SQL com de programació.

En un principi, MySQL no disposava de moltes de les característiques essencials de les bases de dades relacionals, com podien ser la integritat referencial i les transaccions. Però la seva simplicitat va atraure a molts creadors de pàgines web dinàmiques, i, poc a poc, tant desenvolupadors interns com altres de la comunitat del software lliure, han anat incorporant molts elements i característiques entre les que es poden destacar la seva gran disponibilitat en multitud de plataformes, la inclusió de claus externes, la replicació, o la indexació dels camps de text per a disminuir els temps de cerca.

4.2.4 Hibernate

Il·lustració 41: Logo de Hibernate

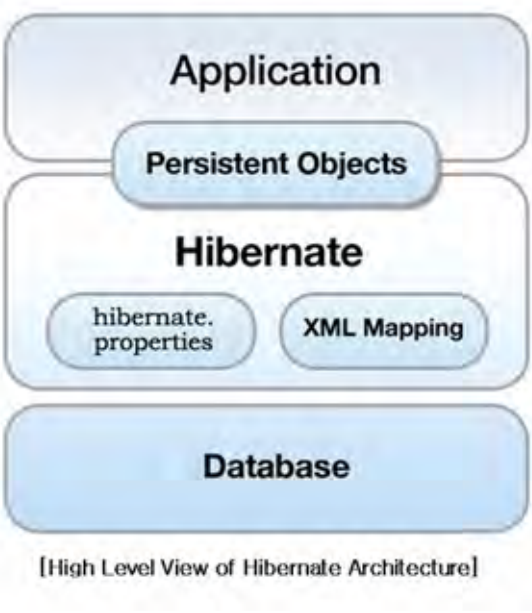
En qualsevol aplicació podem trobar per una banda el **codi**, les instruccions que fan que l'aplicació s'executi seguint uns passos definits, i per un altra, les **dades** que s'estan processant i emmagatzemant. La tècnica que compatibilitza aquestes dues parts en aplicacions de llenguatges orientats a objectes, és el mapatge objecte relacional, o bé **ORM**, per les seves sigles en anglès (**Object Relational Mapping**).

Aquest conflicte s'ha produït per l'evolució dispar que han patit aquestes dues parts de les aplicacions. Al principi, els propis programes accedien directament al disc físic per escriure les dades que s'havien de guardar. Això implicava que el propi programa hagués de disposar de la lògica típica d'una base de dades, necessària per a l'accés, modificació o eliminació de les dades.

Amb el temps es van desenvolupar sistemes per a l'emmagatzematge de les dades, anomenats **Bases de Dades Relacionals**, que permeten la persistència d'entitats, relacions i atributs. La forma d'accedir a aquestes dades és el **Structured Query Language, SQL**, que permet la manipulació de les dades amb un llenguatge proper al llenguatge natural. Aquestes bases de dades tenen una sèrie de regles que permeten mantenir la integritat de les dades, i evitar la redundància. Amb la creació d'aquests sistemes de bases de dades, els propis programes havien d'implementar manualment les consultes SQL que permetien l'accés a la informació que es volia processar i que es trobava a la base de dades.

Però l'evolució dels llenguatges de programació orientats a objectes, on el processament de la informació en memòria de l'ordinador, es realitza manipulant **objectes** dissenyats i instanciats a través del propi llenguatge de programació, generava una **incompatibilitat** entre aquests **objectes**, i els **sistemes de dades relacionals.**

Per tant, s'havia d'aconseguir una "**traducció**" dels objectes a formes que puguin ser emmagatzemades a la base de dades, i que l'accés a les quals sigui ràpid i fàcil, i que preservi les propietats de les taules i les seves relacions. S'aconsegueix així, el que s'anomena **persistència d'objectes**. D'aquesta forma s'aconsegueix una certa **abstracció** de la base de dades, permetent al programador treballar directament amb objectes, i aconseguint una bona integració amb el model vista-controlador.



Il·lustració 42: Funcionament de Hibernate

En la nostra aplicació, el ORM emprat ha estat **Hibernate (**Il·lustració 41), que facilita el mapatge d'atributs de la base de dades relacionals al model d'objectes de l'aplicació mitjançant **fitxers declaratius xml**, o bé **anotacions a les beans de les entitats**, que permeten establir les relacions i restriccions. El desenvolupador pot descriure detalladament com és el seu model de dades, taules, atributs i relacions. **Hibernate** serà l'encarregat de la conversió dels tipus de dades definides en SQL a Java, i de la creació de les sentències SQL per a l'accés a la base de dades. Així, es permet a l'aplicació la manipulació de les dades, operades com a objectes i el programador quedarà alliberat del maneig manual de les dades. Aquesta automatització dóna la capacitat de **portabilitat entre diferents motors de bases de dades** amb un petit increment del temps d'execució (Il·lustració 42).

Hibernate està dissenyat per ser flexible en quant a l'esquema de taules emprat, adaptant-se així a bases de dades existents. També dóna la possibilitat de que la base de dades sigui creada mitjançant la informació declarada a Hibernate. A més ofereix un llenguatge propi de consulta, molt similar a SQL, anomenat **HQL (Hibernate Query Language)** i una API per construir consultes programaticament, coneguda com a "**criteria**".

Hibernate va sorgir de la iniciativa d'un grup de programadors de diferents nacionalitats, i liderats per **Gavin King**. Posteriorment, el projecte fou recolzat per l'empresa Jboss Inc. (comprada per Red Hat) al contractar als principals responsables de Hibernate. Actualment, la versió que s'està desenvolupant és la 3, i la principal novetat és l'ús d'anotacions (en lloc de, o conjuntament amb els fitxers de definició de dades .xml) per definir la correspondència entre les taules de la base de dades i els objectes dels programes. La versió emprada en la nostra aplicació és la 3.3.2.

4.2.5 Maven

Maven (Il·lustració 43) és una **eina per al desenvolupament i control del cicle de vida de projectes en Java** creada per **Jason Van Zyl** per a l'empresa Sonatype a l'any 2002. El seu model de construcció està basat en un format **XML**, i tot i que inicialment formava part del projecte Jakarta, ara es troba a un nivell superior de la Apache Software Foundation.

Il·lustració 43: Logo de Maven

Per a descriure els projectes, les dependències d'altres mòduls, els mòduls externs i l'ordre de construcció de tots els elements, Maven empra un **Project Object Model (POM)**. Moltes tasques estan clarament definides com la compilació de codi o l'empaquetament.

Un dels **problemes més complexes** a l'hora de realitzar projectes **és la gestió de dependències**. **Maven aporta el seu sistema basat en repositoris per intentar solucionar el problema**. La característica principal de Maven és que està dissenyat per treballar en xarxa, i per tant, pot **descarregar dinàmicament els plugins necessaris** d'un repositori d'Internet, el mateix que dóna servei a moltes versions de diversos projectes Open Source en Java, d'Apache i altres organitzacions i desenvolupadors. Aquest repositori i el seu successor reorganitzat, Maven 2, competeix per ser el sistema estàndard de distribució d'aplicacions en Java, però la seva adopció est sent molt lenta. A més de la descàrrega, Maven proveeix suport per a la pujada de dades al repositori al final de la construcció de l'aplicació, permetent l'accés a tots els usuaris.

Maven està construït emprant una **arquitectura basada en plugins**, que li permet emprar qualsevol aplicació controlable a través de l'entrada estàndard. Això permetria, en teoria, que qualsevol desenvolupador pugui crear plugins (compiladors, eines de prova) en qualsevol altre llenguatge a part de Java, però en la pràctica el suport i ús d'altres llenguatges es mínim.

Maven facilita molt el cicle de vida dels projectes que es realitzin amb ell. Des del moment de creació, en que ens proporciona una **estructura de directoris estandarditzada**, fins a la gestió de dependències, l'execució de proves o el desplegament als servidors. Maven organitza els projectes d'una forma estàndard, posant cada arxiu al lloc apropiat per la seva execució, assegurant-nos que el projecte funcionarà correctament. En contrapartida, grans projectes ja existents són molt difícils d'adaptar per a que emprin Maven. Aquest problema s'ha intentat arreglar en la versió Maven 2, fent-lo més configurable.

Maven intenta **estandarditzar** també **el cicle de vida dels projectes**, aportant una implementació a tal efecte, i sense haver de programar res. Executar qualsevol fase del cicle de vida serà igual en tots els projectes Maven, de forma que per a un desenvolupador, aprendre a fer anar un projecte Maven implica que s'ha aprés a fer-los servir tots. A més, aquest **cicle de vida és extensible**, de forma que es poden afegir noves tasques implementades en Java o altres llenguatges.

Maven intenta tenir com a premissa la **reutilització**. Els projectes Java són molt heterogenis, però

normalment utilitzen patrons similars per a la seva construcció, de forma que, sería una elecció lògica reutilitzar aquests processos de construcció. Tot i que Maven és configurable, sempre s'ha emfatitzat en el fet que els usuaris s'adhereixin al seu concepte de model de projecte estàndard tant com sigui possible.

La **integració de Maven amb eines i frameworks és total**, per exemple amb Eclipse, Selenium, CVS o Hibernate. En el nostre cas, l'hem integrat amb Spring Source Tool Suite, i des dels seus repositoris, ens descarrega totes les dependències necessàries per a l'execució del projecte, estalviant-nos haver de configurar-les manualment.

4.2.6 Apache Tomcat

Desenvolupat pel projecte **Jakarta** en la Apache Software Foundation, **Apache Tomcat** (Il·lustració 44) és un **contenidor de Servlets** amb un **entorn JavaServer Pages**. Un **contenidor de Servlets** és una shell d'execució que fa servir servlets invocats per l'usuari. Els servlets són petits programes que corren en un servidor. Generalment són **aplicacions Java**, que corren en un entorn de servidor Web, de forma anàloga a com una aplicació Java corre sobre un navegador. Els Java Servlets s'han tornat molt populars en **substitució dels antics CGI's**. La diferència principal amb els CGI's és la seva **persistència**. Mentre aquests últims desapareixien un cop havien servit a una sol·licitud, els Java Servlets es mantenen en memòria un cop han estat iniciats, i tenen la capacitat de donar servei a diverses sol·licituds, iniciant un fil per cadascuna d'elles. Per aquest motiu, l'execució és més ràpida amb els Java Servlets reduint els recursos de servidor necessaris, i el temps d'execució.

Il·lustració 44: Logo d'Apache

L'especificació original de Servlets, la versió 1.0, fou creada per Sun Microsystems i estava enllestida al Juny de 1997. A partir de la versió 2.3, va ser desenvolupada seguint el Procés de la Comunitat Java (Java Community Process). L'ús més comú dels servlets és generar pàgines web de forma dinàmica a partir dels paràmetres de la petició que envia el navegador web al servidor. Tots els servlets funcionen seguint aquest passos:

- Un servidor carrega i inicialitza el servlet.
- El servlet atén zero o més peticions de client.
- El servidor elimina el servlet.

En primer lloc, el servidor carrega i inicialitza el servlet emprant el seu mètode **init.** La inicialització del servlet estarà completa abans de començar a donar servei a les peticions dels clients. Els servlets no pateixen problemes de concurrència durant el moment de la inicialització, donat que el servidor només crida al mètode **init** al crear la instància, i no serà cridada de nou a no ser que es torni a carregar el servlet. No podrà ser carregat de nou si prèviament no s'ha destruït la instància anterior mitjançant el mètode **destroy**.

Al servidor web no es crearà una nova instància per cada petició de client, si no que, un cop inicialitzat el servlet, aquesta instància començarà a donar servei a les totes peticions, encara que provinguin de diversos clients. Per aquest motiu s'ha de ser especialment curós amb l'accés a variables compartides per evitar problemes de sincronització.

El servlet serà destruït en dos casos. Per tancament del servidor o bé per petició de l'administrador de sistema. Per destruir-lo es crida el mètode **destroy** del propi servlet. Aquest mètode només s'executa un cop, i pot ser invocat inclús quan encara hi hagi peticions de client

esperant resposta. El servidor no executarà de nou el servlet fins que, mitjançant el mètode **init**, el carregui i l'inicialitzi de nou, generant una nova instància del servlet.

Els contenidors de servlets, com Tomcat, es poden classificar en:

- **Contenidors de Servlets Stand-Alone (independents):** són una part integral del servidor web. Seria el cas en que, emprant un servidor web basat en Java, el contenidor de servlets forma part de JavaWebServer (actualment substuït per iPlanet). És el mètode per defecte de Tomcat, però, donat que la majoria dels servidors no estan basats en Java, trobem els següents dos tipus.
- **Contenidors de Servlets dins del procés**: combinació d'un plugin del servidor web, i una implementació de contenidor Java. El plugin del Web Server obre una Màquina Virtual de Java JVM, permetent que el contenidor Java s'executi en ell. Quan una petició vol executar un servlet, el plugin pren el control de la petició, i el passa al contenidor Java utilitzant Java Native Interface. Aquest tipus és adequat per servidors multi-thread d'un únic procés, rendint de forma correcta, però té limitacions en quant a escalabilitat.
- **Contenidors de Servlets fora de procés**: combinació d'un plugin de servidor web, i una implementació de contenidor Java que executa una Màquina Virtual de Java fora del servidor. El plugin del Web Server i la JVM del contenidor empren mecanismes de comunicació entre processos (IPC, InterProcess comunnication), habitualment sockets TCP/IP. Quan una petició vol crear un servlet, el plugin pren el control de la petició, i el passa al contenidor JVM utilitzant IPC's. Millora la escalabilitat i estabilitat respecte als servlets dins de procés, però com a contrapartida, el seu temps de resposta és més elevat.

Tomcat es pot emprar de les dues formes, com a contenidor solitari, o bé com a plugin per a un servidor web. Per tant, sempre que despleguem Tomcat s'ha de decidir com s'utilitzarà, i si no es fa anar com a contenidor solitari, haurem de instal·lar un adaptador de servidor web.

Queda clar, doncs, que Tomcat no és un servidor d'aplicacions com Jboss o JOnAS, si no un contenidor de servlets. A més, inclou un compilador, Jasper, que converteix les JSP's a servlets. El motor de servlets de Tomcat, molt sovint es fa anar en combinació amb el servidor Web Apache. En un principi, existia la creença que Tomcat, com a servidor web autònom no era un opció molt recomanable per a entorns de molt tràfic i alta disponibilitat, així que es feia servir únicament en entorns de desenvolupament amb baixa exigència de velocitat i transaccions. Avui dia aquesta percepció ha canviat, i es fa anar en tota mena d'entorns, i donat que està escrit en Java, funciona amb qualsevol sistema operatiu que disposi de Màquina Virtual de Java.

5 Manual d'usuari

5.1 Introducció

El “Registre Telemàtic de la Diputació de Lleida” és un programa web dissenyat per a la utilització en un entorn d'Administració Pública. La seva funció és l'emmagatzematge de les dades referides als ciutadans de l'àrea adscrita a l'esmentada Administració, així com diversos tràmits burocràtics que qualsevol persona té o pot tenir necessitat de realitzar amb l'Administració. Els tràmits inclosos a l'aplicació són set: el padró d'habitants, la petició de permís d'obra, la llicència per a la realització d'activitats al carrer, la llicència d'ocupació d'edificis o espais públics, les sancions de la guàrdia urbana, la domiciliació dels tributs, i la creació d'una adreça fiscal o de notificacions per a un determinat ciutadà. Aquests tràmits s'han triat aleatòriament consultant altres webs d'administracions públiques, i s'han pres únicament com a mostra representativa de les possibilitats de l'aplicació. Però aquesta aplicació pot ser modificada segons les necessitats del client, afegint els tràmits que es considerin imprescindibles i que en el procés de creació de l'aplicació, no s'hagin tingut en compte.

L`aplicació està dissenyada amb un model client-servidor on les tasques, com el seu nom indica, estan dividides en dos parts. Per una banda, el servidor, que allotjarà una base de dades on s'emmagatzema tota la informació referent als ciutadans, als empleats de l'administració, als tràmits i als documents necessaris per al funcionament de l'aplicació, i el programa servidor per a la recepció de peticions de dades. De l'altra , els clients, que seran els equips dels propis ciutadans, i que faran peticions al servidor per a rebre la informació requerida en cada moment, i que serà enviada pel programa servidor.

L'aplicació està dissenyada com un programa web que podrà romandre online i ser accedida per qualsevol ciutadà des de la comoditat de la seva llar. L'únic requisit serà que el ciutadà, abans de la primera vegada que accedeixi a la web, haurà de donar-se d'alta a l'aplicació. Per fer-ho, caldrà que es personi a l'Administració Pública pertinent. Els treballadors agafaran les dades del ciutadà, i el donaran d'alta a la base de dades. Un cop fet això, el ciutadà ja pot accedir a l'aplicació, per consultar totes les dades referides a ell, de tal manera que la interacció amb l'Administració pugui ser àgil i fluida, i sense necessitat de desplaçaments físics a la seu de l'Administració, únicament la primera vegada per donar-se d'alta.

En aquest punt, cal matisar que un ciutadà pot accedir a l'aplicació de dues formes:

- **Utilitzant l'usuari i contrasenya**: el ciutadà podrà consultar les seves dades personals i els seus tràmits, però no podrà realitzar cap modificació. Qualsevol canvi que es realitzi a les dades, implica ser signat amb el DNI-electrònic. Per tant, si no disposa d'ell, només podrà realitzar consultes, però en cap cas modificacions.
- **Utilitzant el DNI-electrònic**: aquest és el millor mètode d'accés a l'aplicació. El DNI-electrònic garanteix la identitat del ciutadà connectat a l'aplicació, donat que és un document personal i intransferible. Només el propietari del DNI-electrònic coneix el PIN associat al mateix. Per tant, és necessari connectar el DNIe a l'equip client. L'aplicació demanarà automàticament el PIN associat. Un cop introduït correctament, el ciutadà tindrà accés a l'aplicació, i podrà treballa de manera lliure i segura amb totes les seves dades utilitzant totes les capacitats de l'aplicació. Podrà realitzar les mateixes consultes que accedint amb el nom d'usuari i contrasenya, però a més podrà modificar les dades emmagatzemades. Quan ho faci, es generarà una signatura electrònica al registre de la base de dades, utilitzant les claus

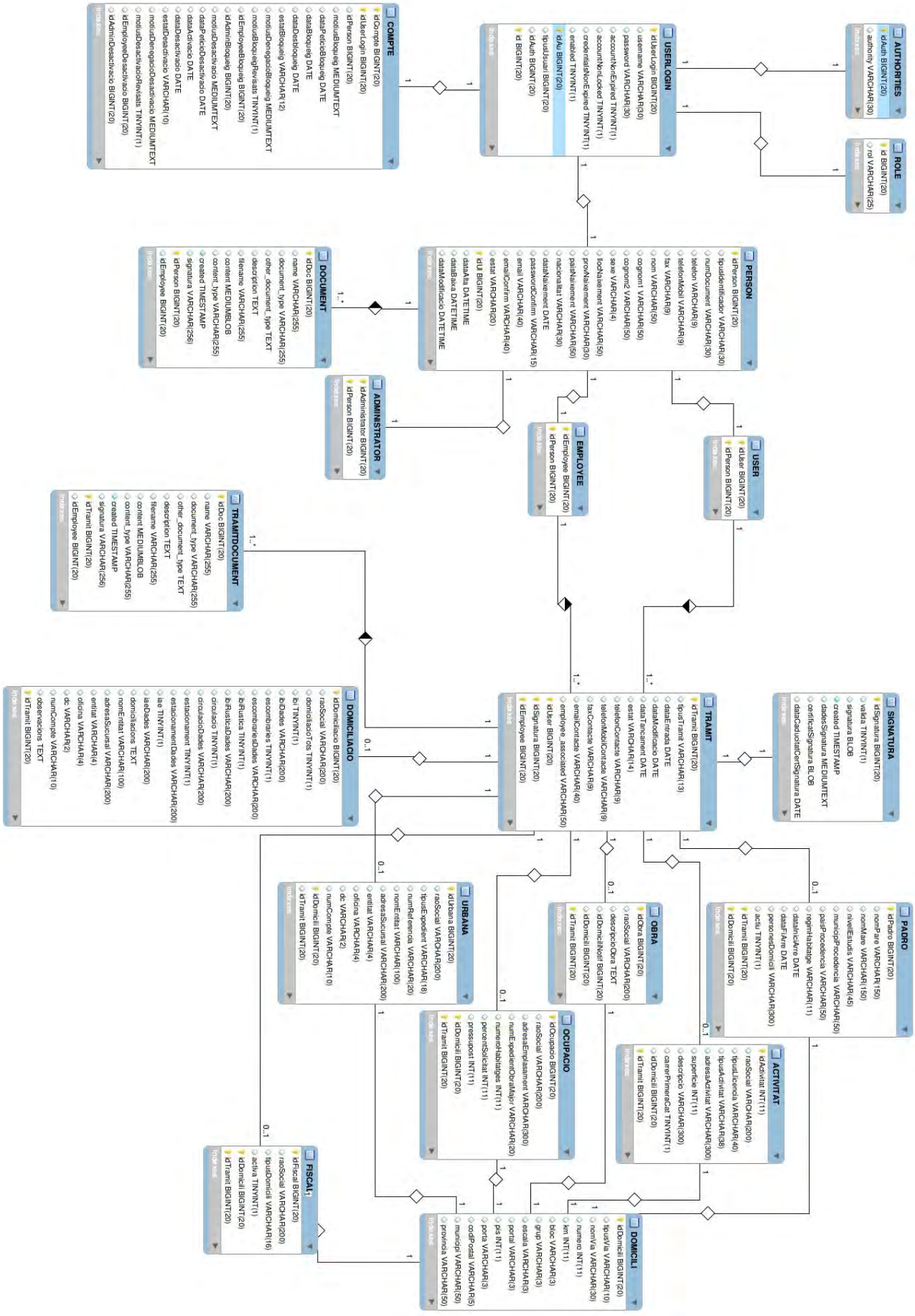
criptogràfiques de les que disposa el Document Nacional d'Identitat. Aquesta signatura no només garanteix que aquestes dades han estat creades per la persona que acredita el DNI-e, sinó que a més garanteix que aquestes dades no han estat modificades a posteriori, i per tant, que les dades que rep l'Administració per part d'un ciutadà, són les que el ciutadà ha escrit i signat.

Podem veure el disseny de la base de dades a la Il·lustració 45. Els diferents tipus de tràmit ("Padró d'habitants", "Permís d'obra", "Sancions de la guàrdia urbana"...) es relacionen amb la taula "Tràmit", que conté la informació comuna a tots els tipus. La taula "Domicili" conté l'adreça de cada tipus de tràmit, amb la peculiaritat que el permís d'obra conté dues adreces, una per la ubicació de la obra en sí, i una altra on enviar les diverses notificacions. El tipus de tràmit "Domiciliació de tributs" no conté una adreça física, donada la manca de necessitat d'aquest informació en aquest cas.

A la base de dades de l'aplicació s'han creat tres tipus d'usuaris diferents. En primer lloc trobem els "usuaris". Aquests fan referència als ciutadans, els usuaris finals de l'aplicació i que faran ús de les capacitats del programa, tant per a la creació com l'emmagatzemament dels tràmits. Com s'ha comentat, aquests usuaris faran servir les capacitats criptogràfiques del DNI electrònic, per tal d'assegurar la identitat del ciutadà, i la integritat de les dades enviades a l'aplicació. Un "usuari", o ciutadà només té accés a les seves dades personals i d'accés a la web, així com els seus tràmits. També trobarem els "empleats". Com el seu propi nom indica, aquests usuaris fan referència als treballadors de l'Administració Pública que empra l'aplicació per a donar servei als ciutadans. Aquests "empleats" tenen accés a diverses funcionalitats que queden fora de l'abast dels ciutadans, o "usuaris". Per exemple, tenen la capacitat d'anul·lar determinats tràmits, consultar la informació de qualsevol ciutadà que estigui donat d'alta a l'aplicació, i inclús les dades que hagin estat introduïdes i gestionades per altres empleats de l'Administració, tenint com a finalitat l'agilitat en el servei als ciutadans en el cas que un determinat empleat no pugui desenvolupar les seves funcions per qualsevol motiu. Els empleats poden modificar totes les dades tant dels usuaris com dels tràmits que s'emmagatzemen a la base de dades. S'ha de tenir en compte que, si un "empleat" modifica les dades que han estat enviades i, prèviament, signades per un ciutadà, aquesta signatura deixarà de ser vàlida, donat que la signatura s'haurà realitzat a partir d'unes dades que ja no són les que l'usuari havia introduït inicialment. Per aquest motiu, quan es produeixi aquesta situació, l'"usuari" serà advertit de la situació, quan accedeixi a l'aplicació, i serà instat a signar les dades novament. D'aquesta forma quedarà garantida la integritat de les dades, que seran revisades de nou pel ciutadà. Finalment, trobem un tercer tipus d'usuaris, els "administradors". Aquests seran els membres executius de l'Administració Pública, i la seva funció en l'entorn de l'aplicació serà donar validesa als perfils dels empleats, així com a algunes de les seves accions, que requeriran l'aprovació per part dels "administradors".

Tots els tipus d'usuari de la base de dades es relacionen amb la taula "Person", que conté les dades comunes a tots els tipus d'usuari. Aquesta taula es relaciona amb diverses taules ("Authorities", "Role", "UserLogin" i "Compte") que contenen la informació relativa als comptes d'usuari dels diferents usuaris introduïts a la base de dades de l'aplicació per gestionar els seus perfils d'usuari i les tasques per ales quals estan autoritzats.

Finalment trobem dues taules, "Document" i "TramitDocument" que emmagatzemaran diferents fitxers que contindran documentació relativa als usuaris i als tràmits respectivament. Seran aquestes dues taules les que permetran la funcionalitat de Gestor documental" (5.2.5 Gestor documental per als "empleats", i 5.3.5 Gestor documental per als "usuaris") de la que parlarem en profunditat més endavant en aquest manual d'usuari.



Il·lustració 45: Model entitat relació de la base de dades

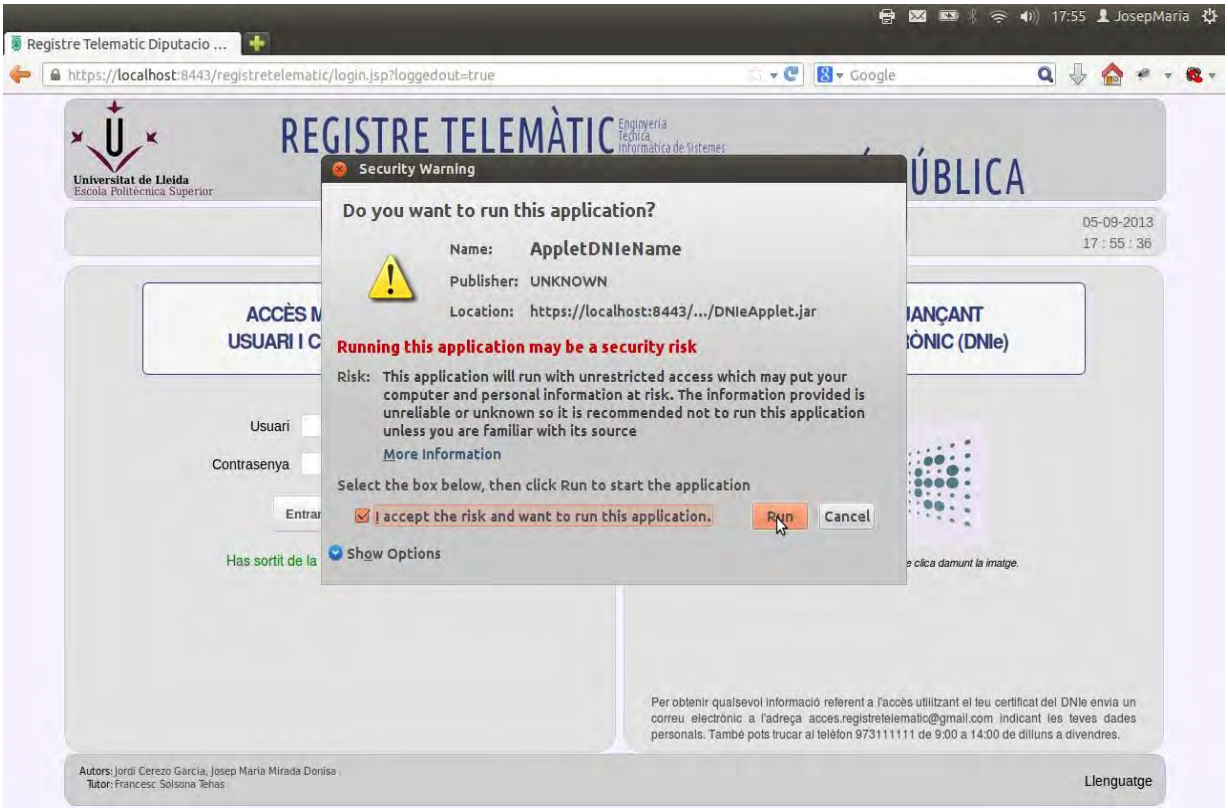
Aquest manual d'usuari s'ha creat separant aquests usuaris, ja que les funcions que realitza cadascun d'ells són diferents. D'aquesta manera, cada usuari podrà conèixer les seves capacitats i possibilitats al programa, i restarà en mans de l'Administració Pública corresponent, posar en coneixement de cada usuari només la informació referent al seu rol a l'aplicació, o bé el manual d'usuari complet. La pantalla d'accés a l'aplicació (Il·lustració 46) ens mostra el títol de l'aplicació, la data i l'hora, el correu electrònic i telèfon i l'horari de contacte, i les dues possibles vies d'accés al programa, mitjançant el nom d'usuari i contrasenya, o bé mitjançant el DNI-electrònic. A la part inferior dreta de la pantalla de benvinguda, es troba l'enllaç anomenat "Llenguatge". Aquest botó forma part del peu de l'aplicació, de manera que serà visible en tot moment mentre el programa estigui sent executat. En ser pres, aquest botó desplegarà tres opcions diferents d'idioma, el català, el castellà, o bé l'anglès. Si l'usuari prem un d'aquest botons, l'aplicació modificarà el seu idioma, mostrant-se en pantalla tots els missatges disponibles per la interacció amb l'usuari en l'idioma escollit. Si es prem el botó de l'idioma que actualment està mostrant-se en pantalla, no es produiran canvis. Aquest manual d'usuari ha estat creat mostrant totes les pantalles en idioma català.

Il·lustració 46: Pantalla d'accés de l'aplicació

Si en l'accés a l'aplicació es produeix un error, és a dir, si el nom d'usuari i contrasenya introduïts, o bé el PIN del DNI-electrònic són incorrectes, l'aplicació retornarà a la pantalla inicial, mostrant un missatge informant sobre el problema causant de l'error a l'usuari (Il·lustració 47). Si el nom d'usuari i contrasenya, o bé el PIN del DNI-electrònic són correctes, l'aplicació comprovarà el tipus d'usuari al qual corresponen les dades, i obrirà el menú principal, mostrant les opcions corresponents al tipus d'usuari connectat.

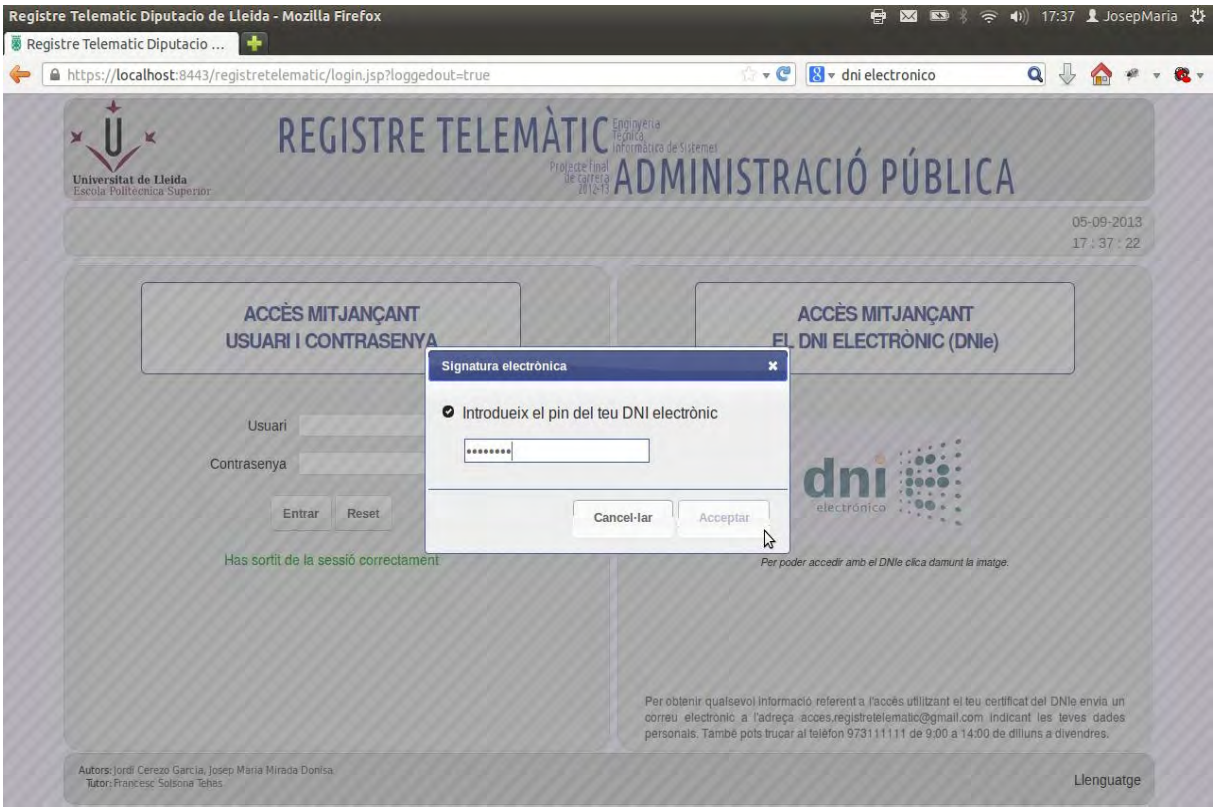
Il·lustració 47: Pantalla d'accés mostrant error d'accés

Si l'accés es realitza mitjançant el **DNI-electrònic**, l'usuari haurà de connectar-lo al lector de l'equip. Inicialment l'aplicació demanarà confirmació per a l'execució de l'applet del DNIe (Il·lustració 48).



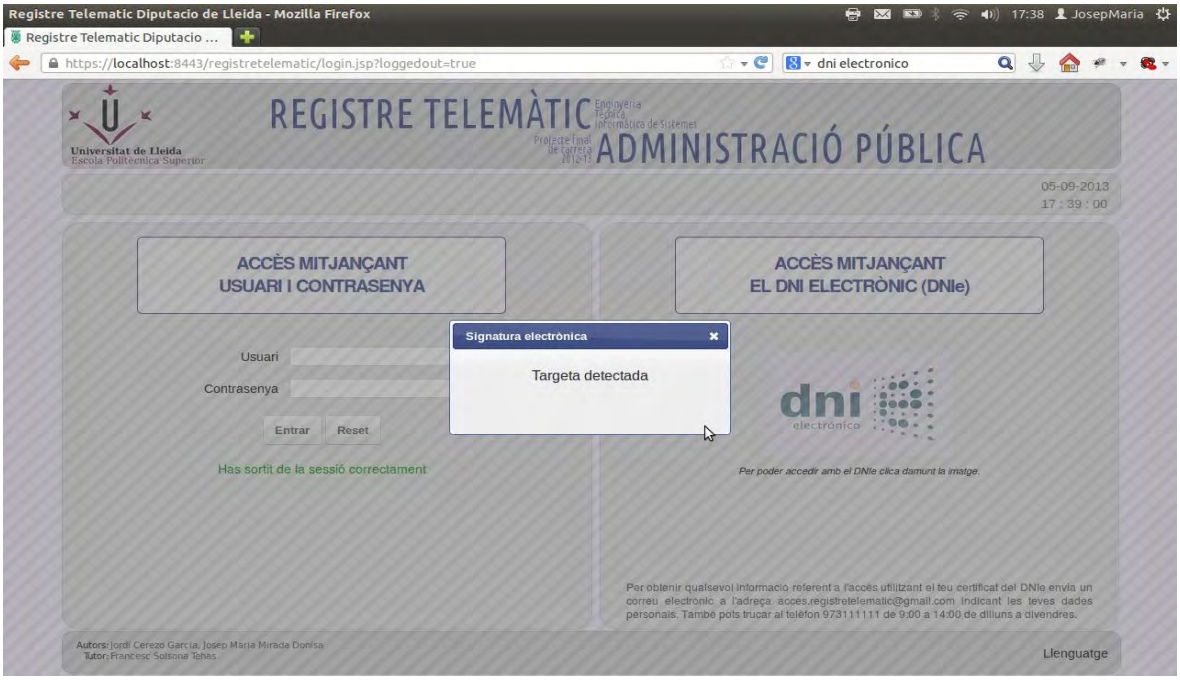
Il·lustració 48: Accés a la web amb DNI-e. Petició de confirmació de l'execució de l'applet.

Un cop acceptada l'execució, es mostrarà un diàleg en pantalla que demanarà a l'usuari el PIN del seu DNIe (Il·lustració 49).



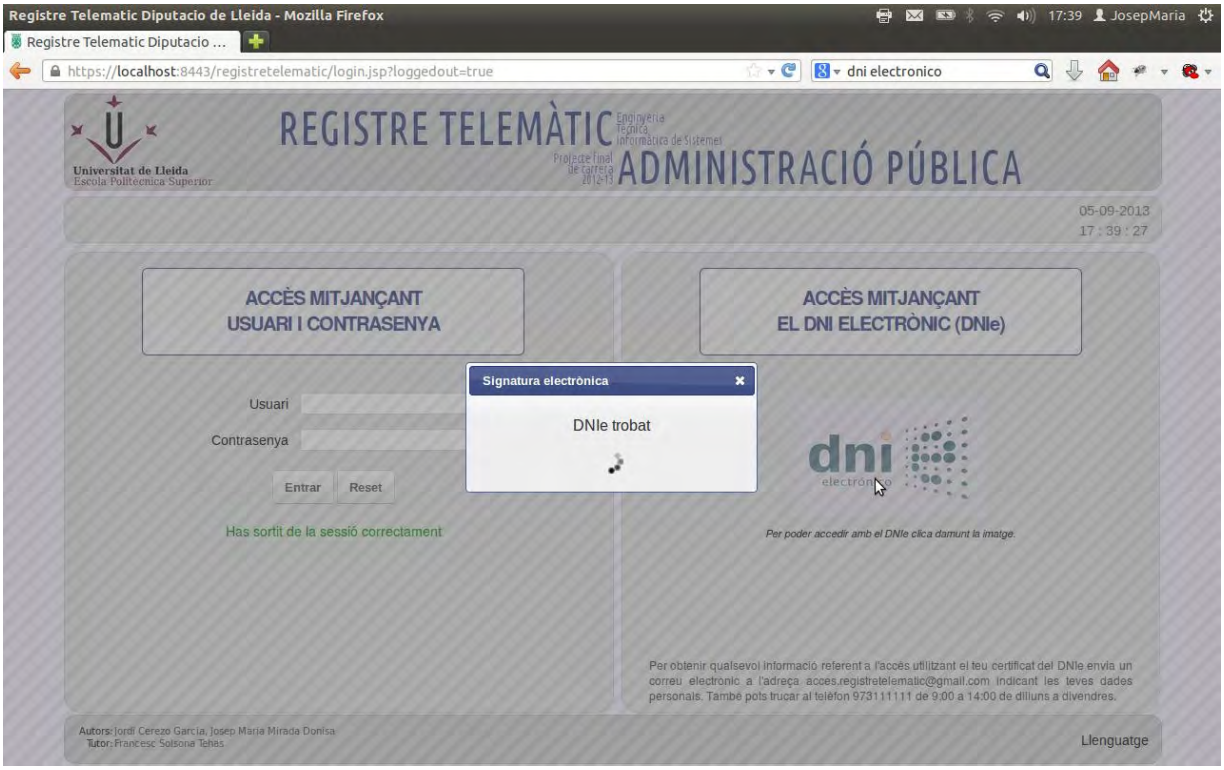
Il·lustració 49: Accés a la web amb DNI-e. Petició de PIN.

Si el PIN és correcte, el següent pas que realitzarà l'applet serà comprovar si hi ha inserida una targeta al lector (Il·lustració 50).



Il·lustració 50: Accés a la web amb DNI-e. Detecció de targeta.

Si l'applet detecta una targeta inserida, comprovarà que sigui un DNIe (Il·lustració 51).



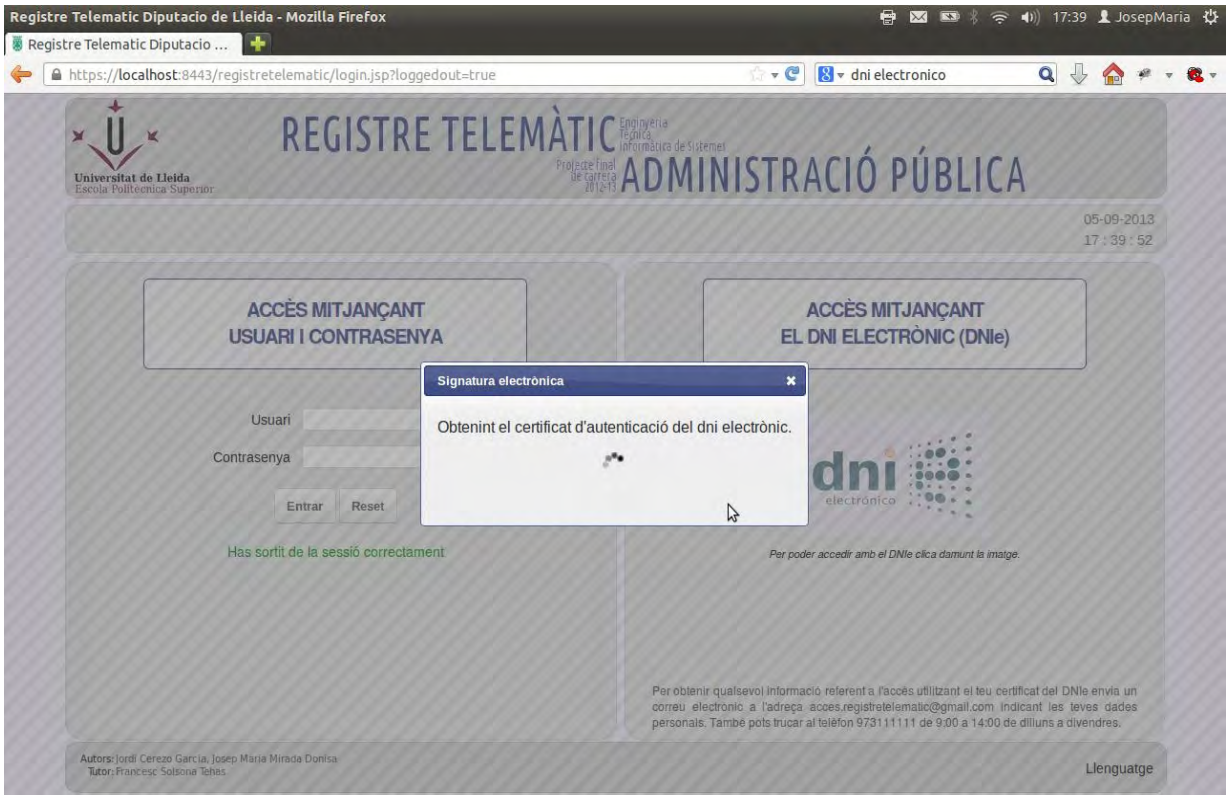
Il·lustració 51: Accés a la web amb DNI-e. Detecció de DNI-e.

Java voldrà bloquejar de nou l'execució de l'applet del DNI-e, donat que detecta que el codi és potencialment perillós (Il·lustració 52).

Il·lustració 52: Accés a la web amb DNI-e. Petició de bloqueig.

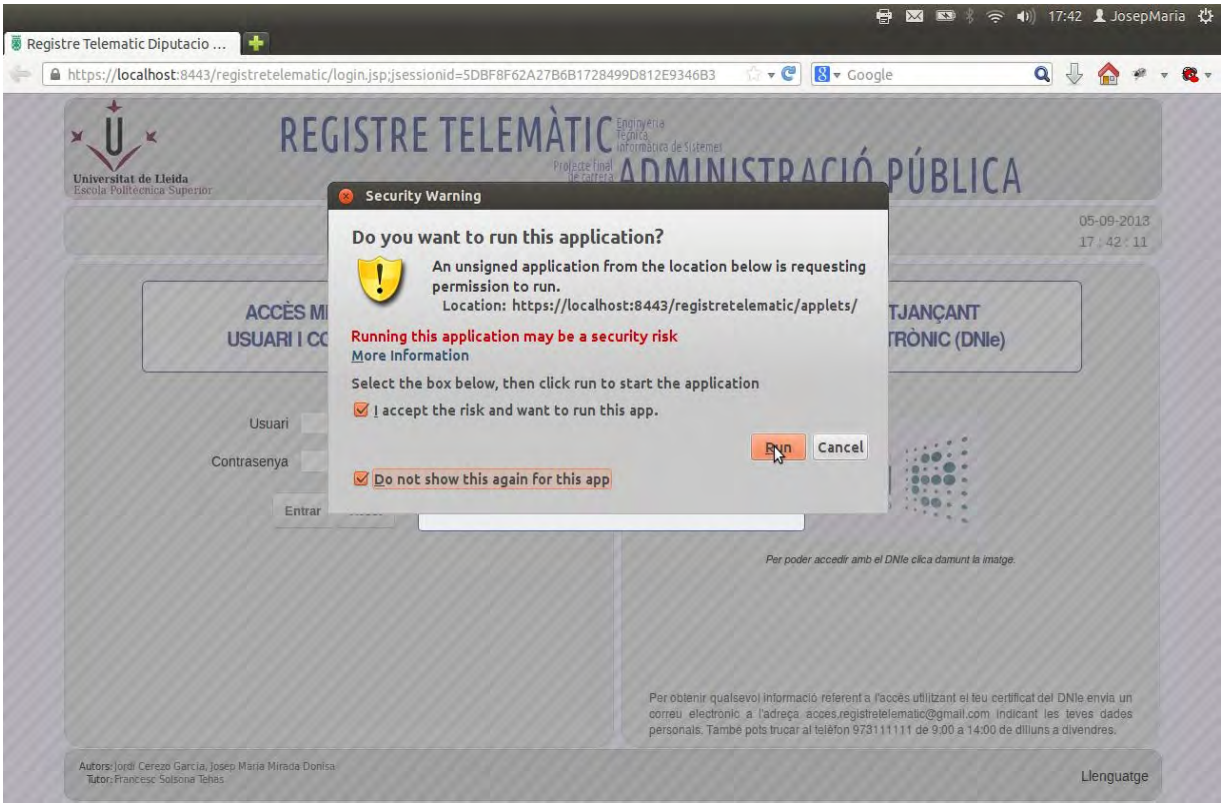
En aquest cas, el ciutadà haurà de negar aquest bloqueig, ja que confia en el software posat a la seva disposició per part de l'Administració.

L'applet obtindrà a continuació el certificat d'autenticació que conté el DNIe (Il·lustració 53).



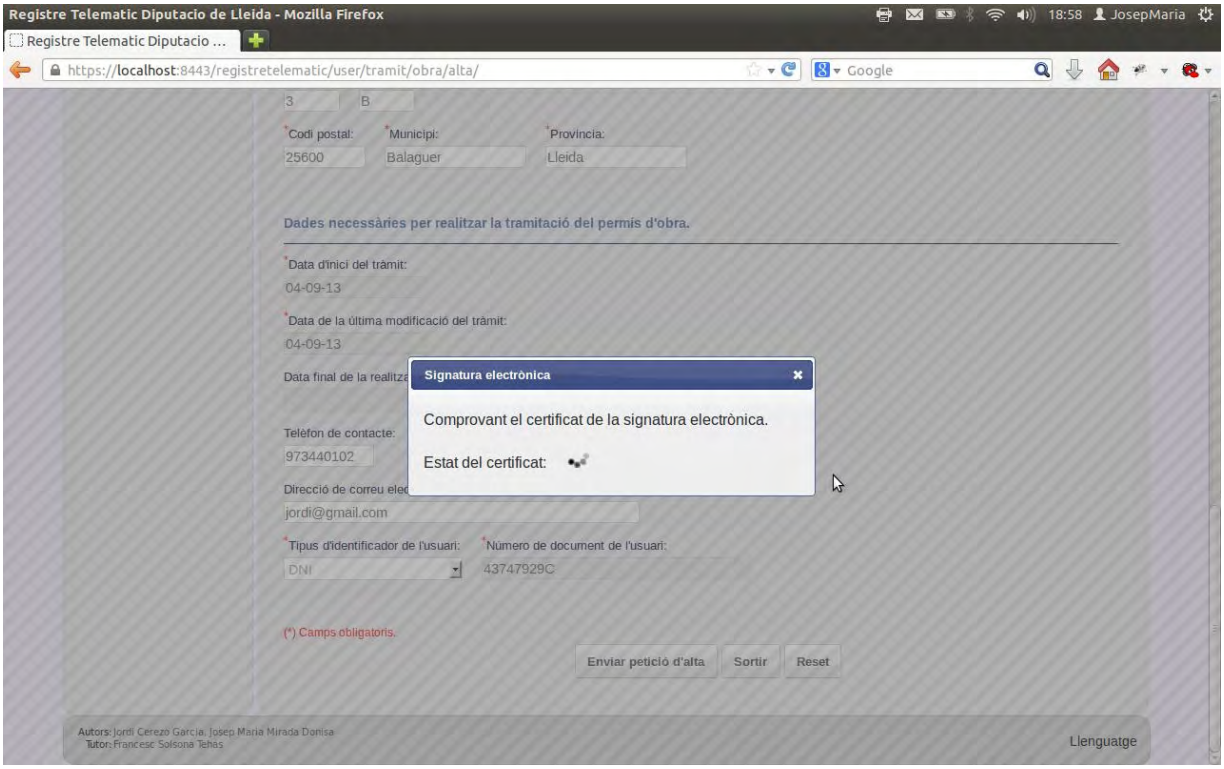
Il·lustració 53: Accés a la web amb DNI-e. Obtenció de certificat.

Java demanarà de nou confirmació per a l'execució de l'aplicació d'autenticació (Il·lustració 54).



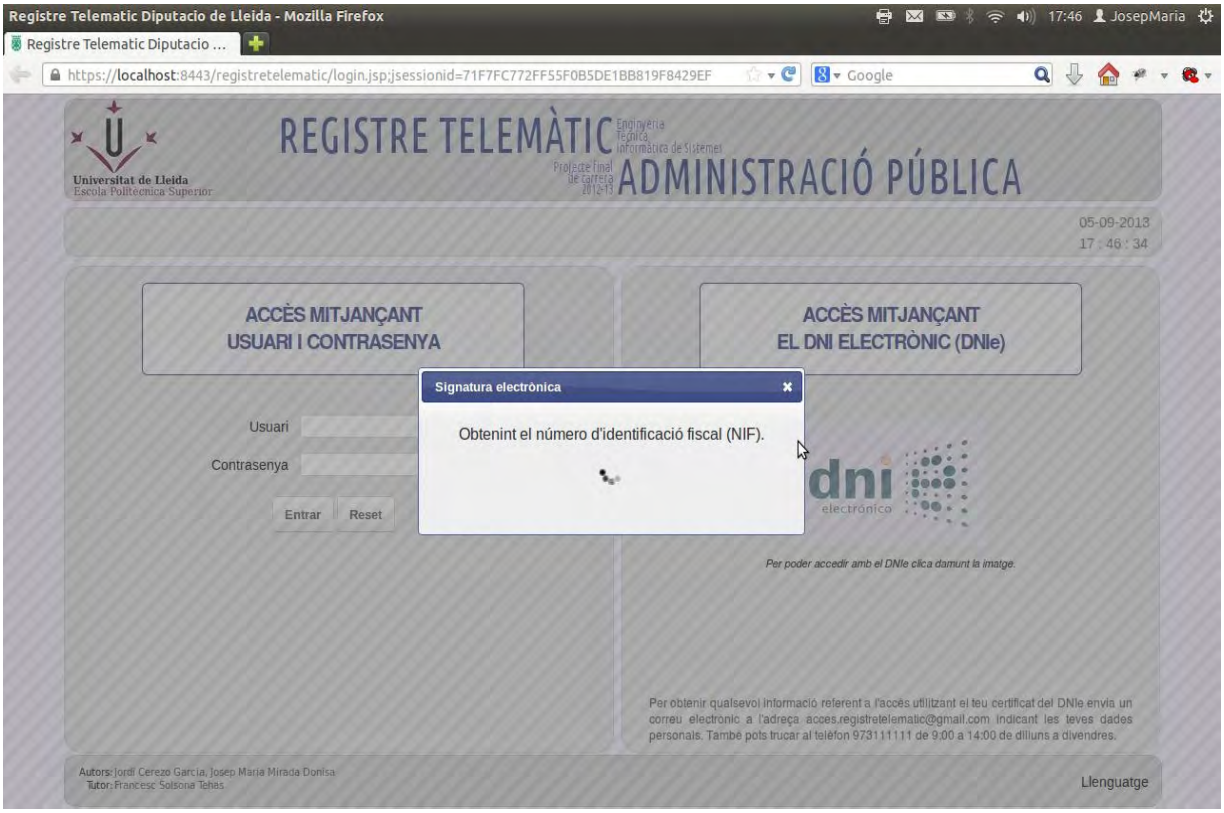
Il·lustració 54: Accés a la web amb DNI-e. Petició de confirmació d'execució.

Tot seguit, es comprovarà la validesa del certificat d'autenticació obtingut (Il·lustració 55):



Il·lustració 55: Accés a la web amb DNI-e. Comprovacio d'estat del certificat d'autenticació.

Si l'estat del certificat d'autenticació és vàlid, l'applet obtindrà el número d'identificació fiscal del titular del DNIe (Il·lustració 56)



Il·lustració 56: Accés a la web amb DNI-e. Obtenció de número d'identificació fiscal.

Si alguns dels passos d'aquest procés falla, l'aplicació mostrarà un missatge d'error retornant a la pantalla d'accés a la web. Si, en canvi, tots els passos són correctes, l'usuari accedirà normalment a l'aplicació, i podrà realitzar qualsevol de les tasques assignades al seu perfil d'usuari.

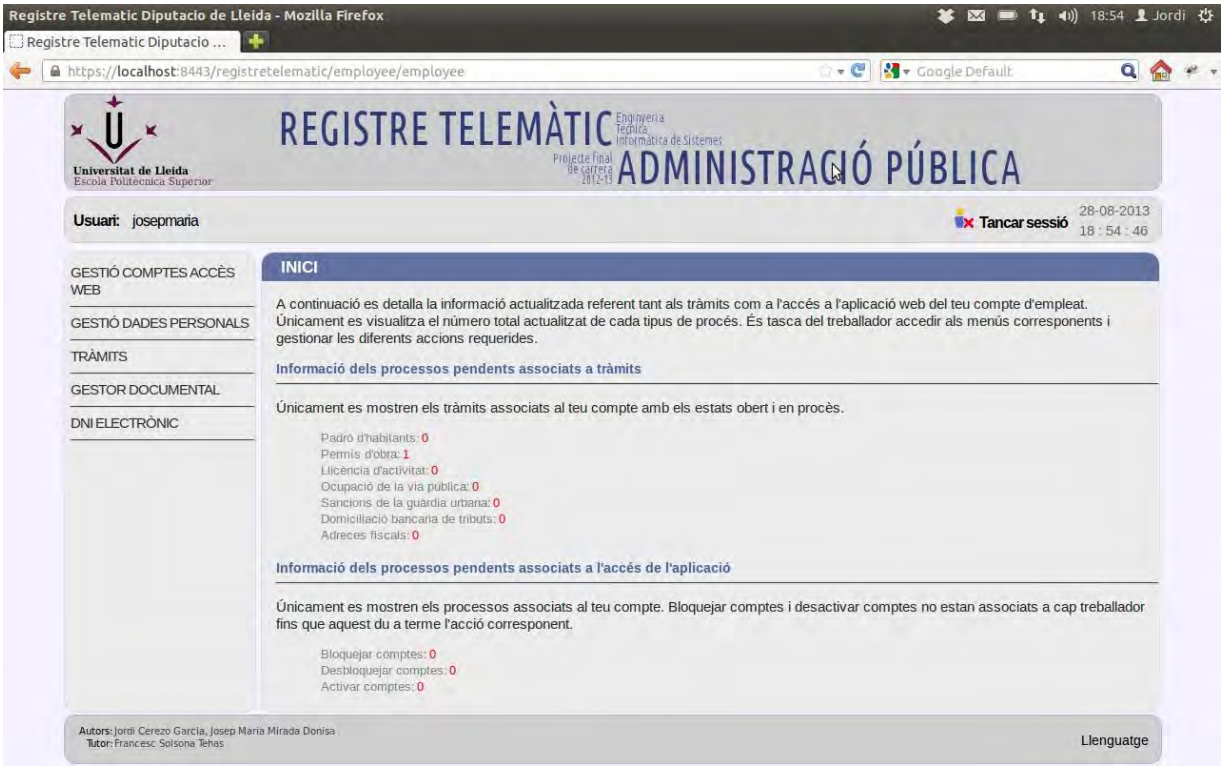
5.2 Empleat

5.2.1 Pantalla inicial

En la pantalla inicial (Il·lustració 57) de l'aplicació per a l'empleat, trobem un menú a la part esquerra, que serà el mètode d'accés a totes les possibilitats que ens proporciona el programa de registre telemàtic. Navegant per aquest menú podrem realitzar totes aquelles tasques necessàries per a la creació, emmagatzemament, consulta i modificació de les dades necessàries per al bon funcionament de l'aplicació. Entre les més importants trobem la gestió de les dades dels usuaris de l'aplicació, i la gestió dels tràmits disponibles a l'Administració Pública corresponent, i de la documentació associada a aquests tràmits, i que també poden ser desats a la base de dades de l'aplicació.

En aquesta pantalla inicial es mostren una sèrie d'estadístiques que permeten a l'empleat, immediatament al accedir a l'aplicació, saber quines són les tasques pendents de realitzar. En primer lloc es mostren quins són els tràmits que estan pendents de ser revisats per l'empleat. Es mostren separats segons el tipus de tràmit. Per fer-ho, l'empleat s'haurà d'adreçar al menú contextual, a l'entrada “Tràmits”. Un cop els revisi, i en doni el vist-i-plau, seran validats i admesos a l'aplicació com a correctes. Si en revisar-los, l'empleat troba algun problema amb les dades proporcionades pel ciutadà al tràmit en qüestió, aquest no serà validat. En aquest cas, l'empleat hauria de posar-se en contacte amb el ciutadà que ha creat el tràmit per tal que les dades siguin corregides. Inclús si l'errada és trivial, i pot ser solucionada per l'empleat, s'haurà d'avisar al ciutadà de la modificació, per tal que signi electrònicament, mitjançant el DNI-e, les dades corresponents al tràmit tractat.

En segon lloc es mostren estadístiques sobre els processos pendents, pel que es refereix a les dades d'accés dels usuaris a l'aplicació. L'empleat haurà de revisar quins comptes d'usuaris han estat bloquejats o desactivats darrerament, i donar el seu vist-i-plau als canvis produïts. Per fer-ho, l'empleat haurà de fer ús del menú contextual, i adreçar-se a l'enllaç de “Gestió de comptes accés Web”.



Il·lustració 57: Pantalla inicial de l'empleat

També podem observar en aquesta pantalla inicial de l'aplicació web, el botó anomenat “Tancar Sessió”. Com indica la seva etiqueta, aquest botó serveix per tancar la nostra sessió a l'aplicació, i retornar-nos a la pantalla d'accés al programa, on es pot introduir el nom d'usuari i contrasenya, o bé el DNI-e, i el seu PIN.

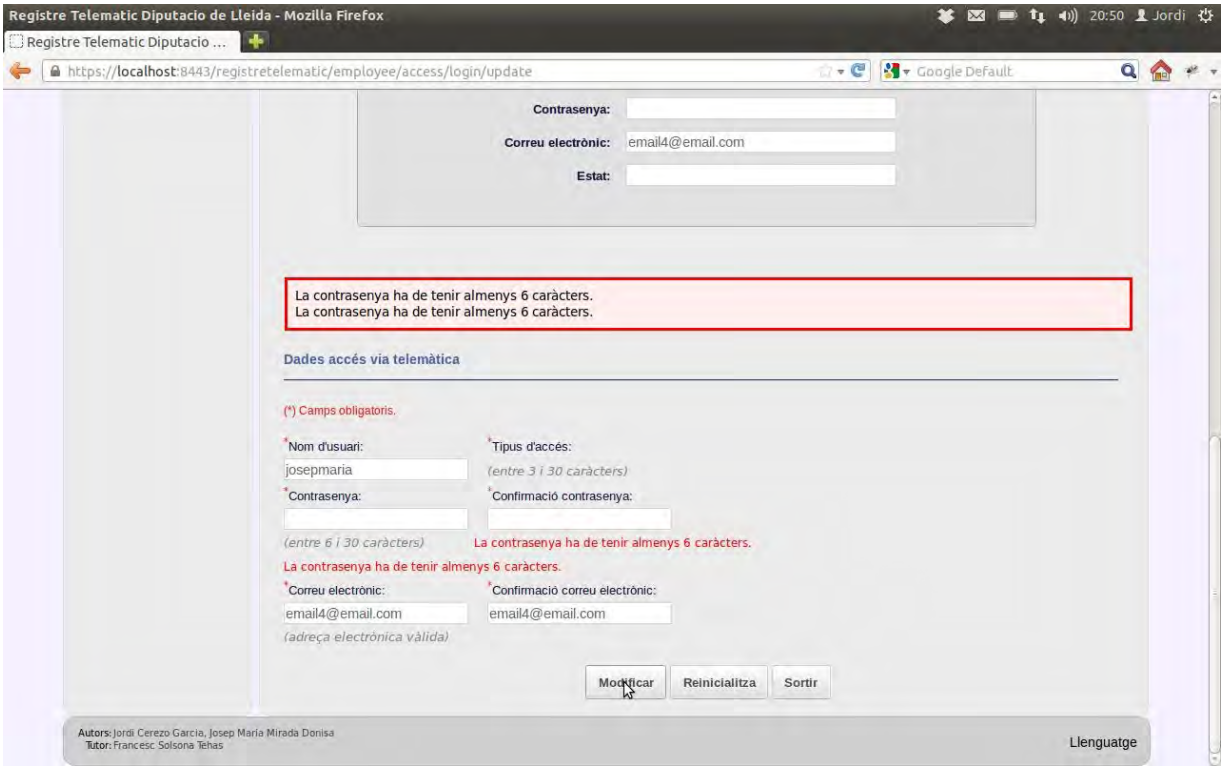
5.2.2 Gestió de comptes d'accés web

La primera entrada del menú lateral (Il·lustració 58), ens permetrà la **“Gestió dels comptes d'accés a la web”** del programa, és a dir, la gestió dels comptes d'usuaris que tenen accés a l'aplicació. En prémer aquest botó, es desplegarà el menú associat amb una sèrie d'entrades que ens faciliten l'esmentada gestió. Tot seguit passem a veure-les més detalladament.

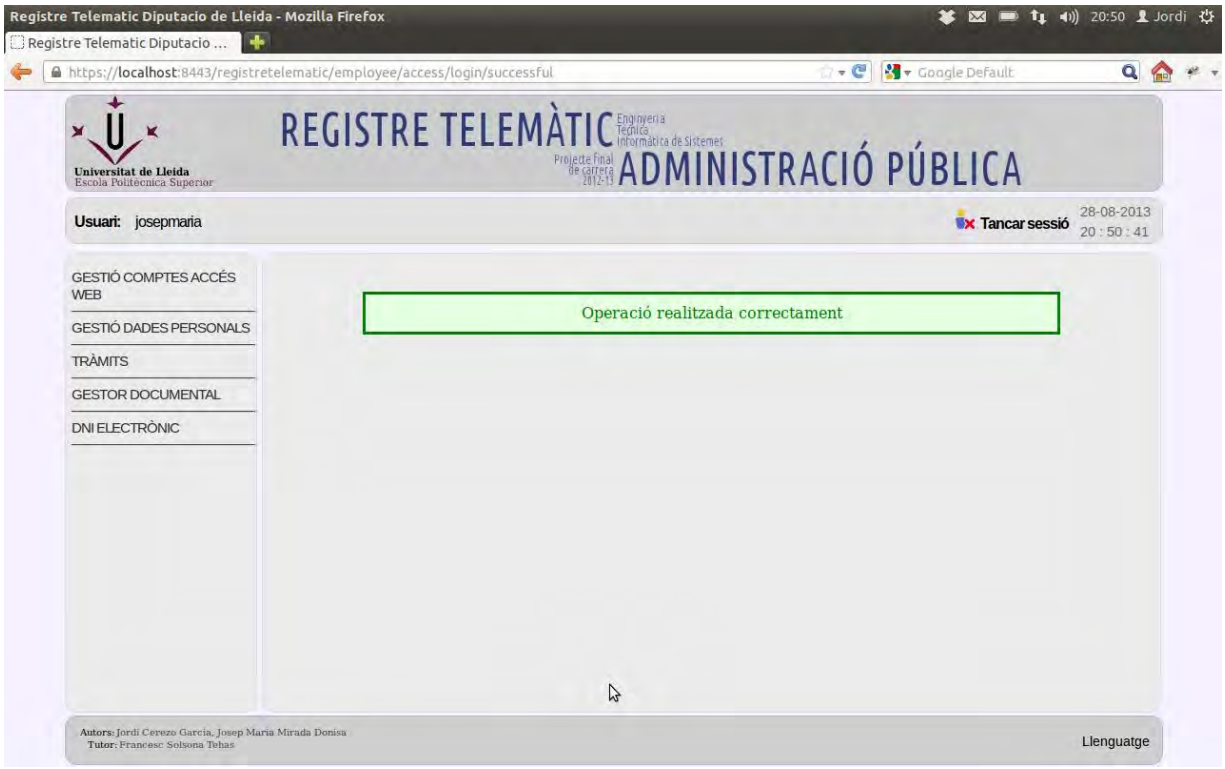
Il·lustració 58: Gestió de comptes d'accés web

5.2.2.1 El meu compte d'accés web

En prémer aquest botó, es desplegaran dues noves opcions en pantalla. La primera, etiquetada com **"Consultar i modificar el meu nom d'usuari i contrasenya"**, ens permetrà la consulta i modificació de les dades del nostre compte d'accés a la pàgina web. A la part superior es mostren les dades de la persona associada al compte web, i a la part inferior, les dades del compte d'accés. Aquestes són les dades que poden ser alterades. Per tal de fer-ho, s'han d'escriure les noves dades a les caixes de text, i prémer el botó "Modificar". Si les dades són incorrectes, es mostrarà un missatge d'error a la vora de les caixes de text on s'ha detectat l'error informant a l'usuari del problema (Il·lustració 59). Si les dades no presenten cap error, es mostrarà un missatge informant de la correcta modificació (Il·lustració 60).

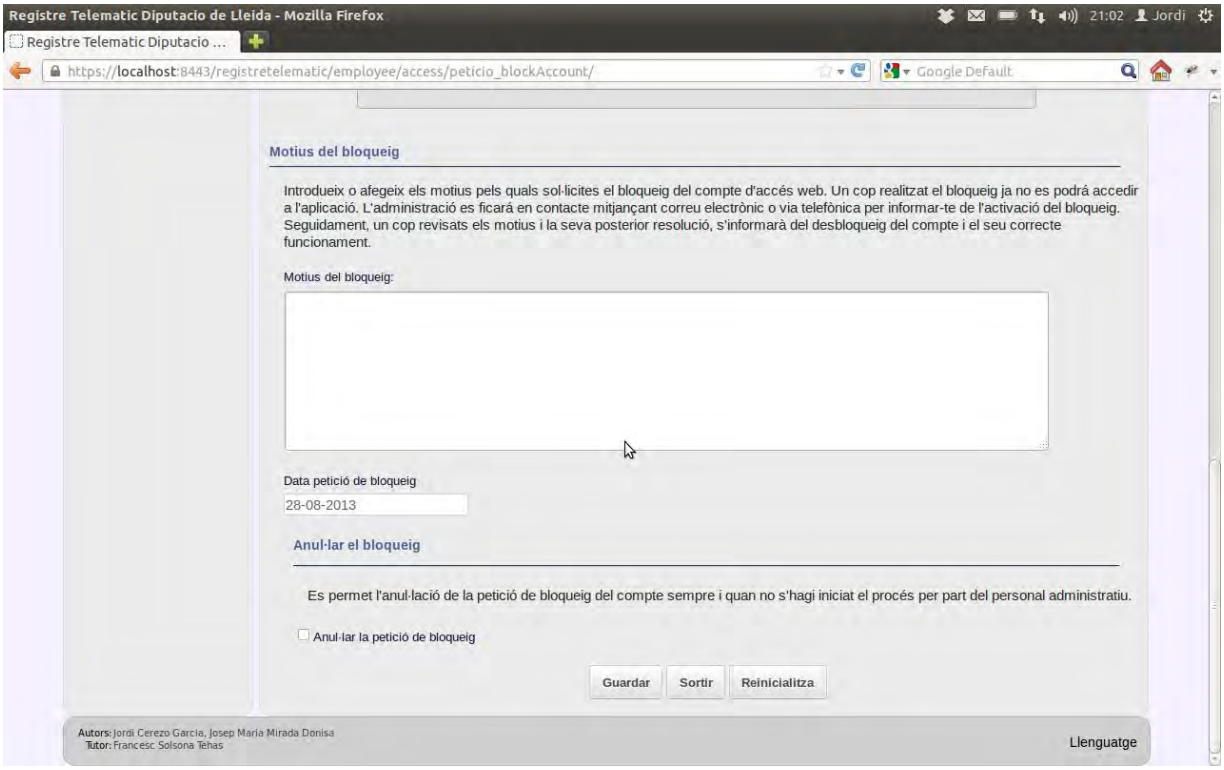


Il·lustració 59: Gestió del meu compte web mostrant un error a les dades introduïdes



Il·lustració 60: Gestió del meu compte web mostrant l'èxit en la operació de modificació

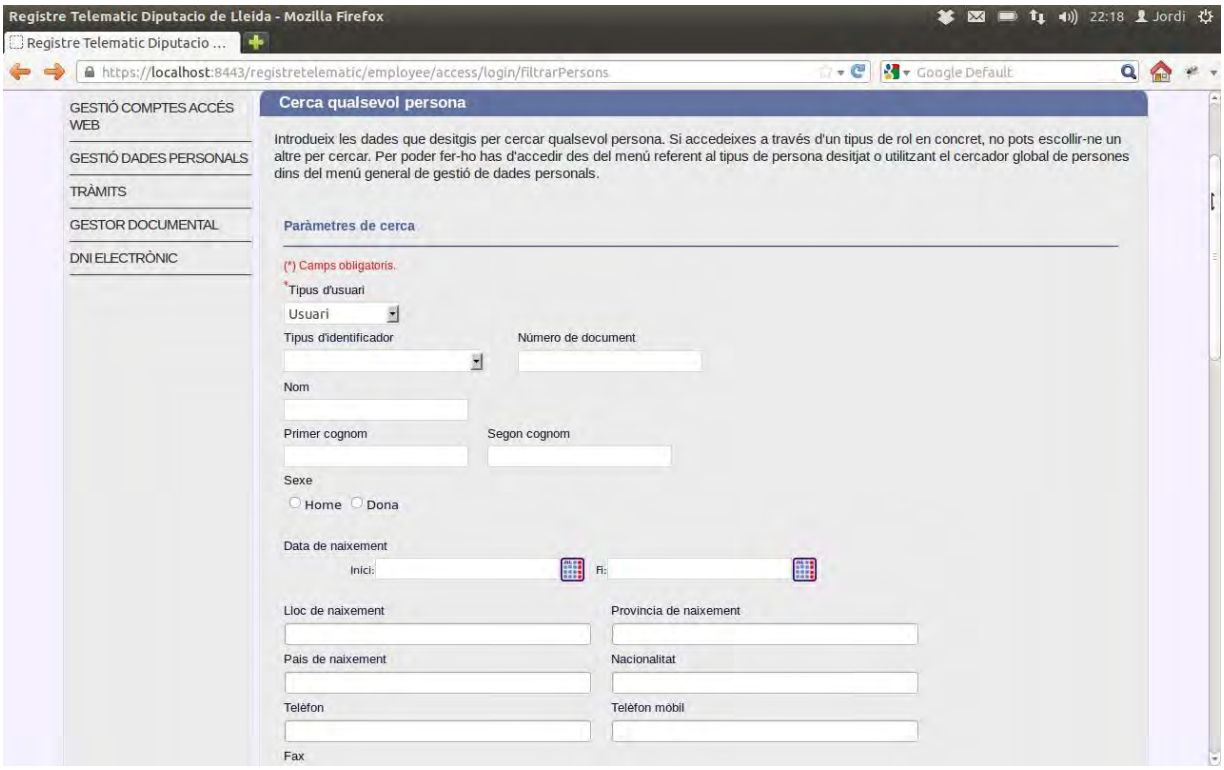
El segon botó etiquetat com a **“Bloquejar el meu compte”** permet bloquejar el propi compte de l'empleat que ha iniciat sessió a l'aplicació (Il·lustració 61). A la part inferior de la pantalla es demanen els motius pels quals es vol donar de baixa el compte, cosa que es realitza prement el botó “Guardar”. També és visible un checkbox que permet, activant-lo, anul·lar una petició de bloqueig, sempre que el procés no hagi estat iniciat pel personal administratiu de l'Administració.



Il·lustració 61: Bloqueig del propi compte de l'empleat

5.2.2.2 Consultar i modificar usuaris i/o contrasenyes

El segon botó del menú de **“Gestió de comptes d'accés web”** ens adreça directament a un cercador de persones (Il·lustració 62), els quals es troben a la base de dades de l'aplicació.



Il·lustració 62: Cercador de persones per consultar i modificar comptes d'accés web

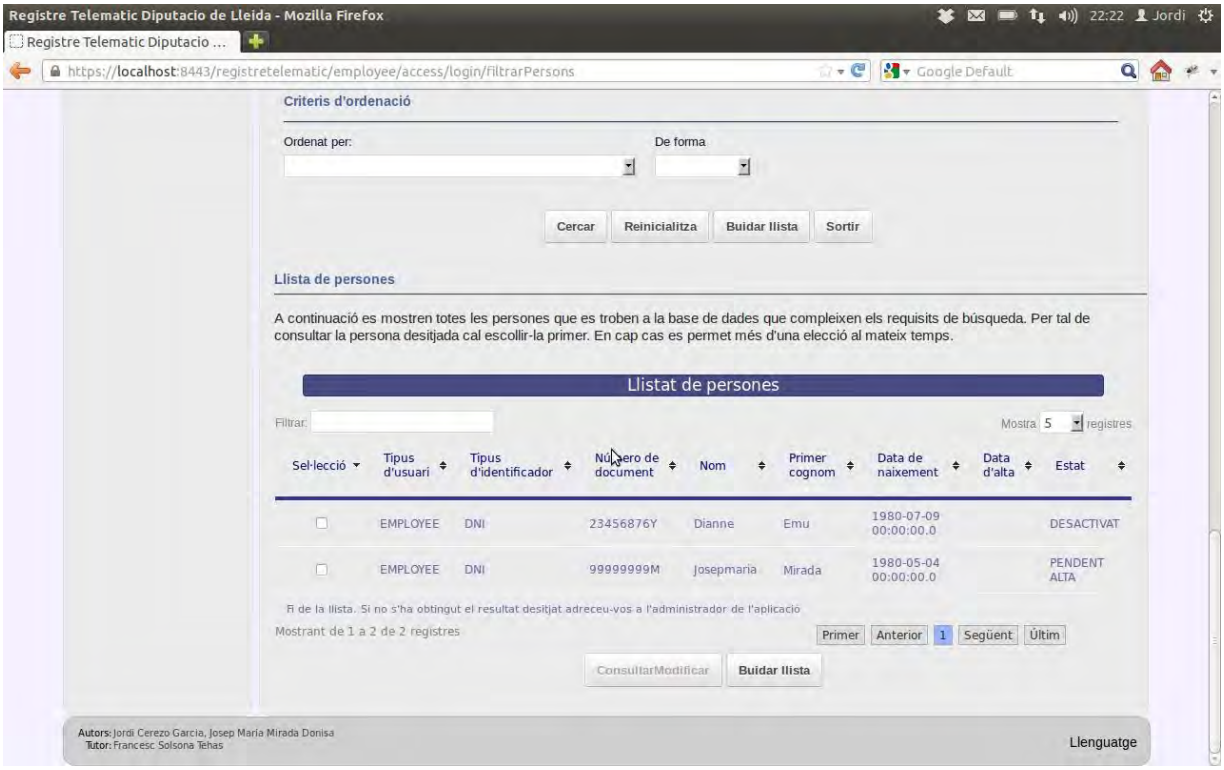
Aquesta pàgina permet realitzar una cerca de persones, filtrant els resultats per tots aquells paràmetres que es troben en pantalla, i mostrant els resultats a la taula de la part inferior:

- **Tipus d'usuari**: permet escollir el tipus d'usuari a cercar, administrador, empleat o usuari. Si es deixa en “Qualsevol”, es cercarà per tots els tipus d'usuari.
- **Tipus d'identificador/Número de document**: permet triar el tipus de document mitjançant el qual la persona es va identificar per donar-se d'alta a l'aplicació, i el número d'aquest document.
- **Nom i cognoms**: permet cercar segons el nom i cognoms de l'usuari. La cerca es realitza per comparació de cadenes de text, de tal manera que, si només coneixem una part del nom, podem escriure només aquella part, i l'aplicació cercarà els usuaris que continguin aquella part.
- **Sexe**: segons si és home o dona. Si no es marca un dels dos, aquest paràmetre no es tindrà en compte (es mostraran els usuaris d'ambdós sexes).
- **Data de naixement**: l'aplicació permet acotar la data de naixement a dues dates concretes. Si no s'emplenen aquests camps, el paràmetre no es tindrà en compte. Si només es plena la data d'inicial, es mostraran les persones amb data de naixement posterior a la introduïda. Si només es plena la data final, es mostraran les persones amb data de naixement anterior a la introduïda.

- **Lloc de naixement**: permet buscar persones nascudes a una localitat concreta.
- **Província de naixement**: permet buscar persones nascudes a una província concreta.
- **País de naixement**: permet buscar persones nascudes a un país concret.
- **Nacionalitat**: permet buscar persones d'una nacionalitat concreta.
- **Telèfon**: permet buscar persones segons el seu telèfon.
- **Telèfon mòbil**: permet buscar persones segons el seu telèfon mòbil.
- **Fax**: permet buscar persones segons el seu fax.
- **Clau d'accés web**: permet cercar segons la seva contrasenya.
- **Estat**: permet cercar segons l'estat del compte a la base de dades.

És possible també realitzar una ordenació dels resultats segons qualsevol dels paràmetres presents al desplegable “Ordenat per:”, i disposar-los de manera ascendent o descendent. Per realitzar la cerca, s'ha de prémer el botó **“Cercar”**. El botó **“Reinicialitza”** restaura tots els camps del cercador al seu estat per defecte. El botó **“Buidar llista”** permet buidar la llista de la taula inferior, corresponent a la darrera cerca realitzada. El botó **“Sortir”** ens porta directament a la pantalla inicial de l'aplicació.

La llista de la part inferior de la pantalla contindrà, com s'ha esmentat anteriorment, els resultats de la la darrera cerca realitzada (Il·lustració 63). Aquesta taula té diverses funcionalitats pròpies. A la part superior esquerra hi ha una caixa de text mitjançant la qual es poden filtrar els resultats de la taula, amb la finalitat d'afinar encara més la cerca. A la part superior dreta es pot introduir el número de registres que es volen mostrar a cada pàgina de la taula. A la part inferior dreta hi ha una sèrie de botons que permeten la navegació a través dels registres de la taula, portant a l'usuari de forma directa a la primera pàgina, la pàgina anterior, la pàgina següent, la pàgina final, i qualsevol d'elles de manera directa, mitjançant el seu número. ***Totes les taules de resultats de l'aplicació tenen la mateixa funcionalitat, per tant, en totes les pantalles que mostrin un llistat d'ara en endavant en aquest document, obviarem l'explicació del funcionament de la taula, i la navegació pels registres mostrats.***

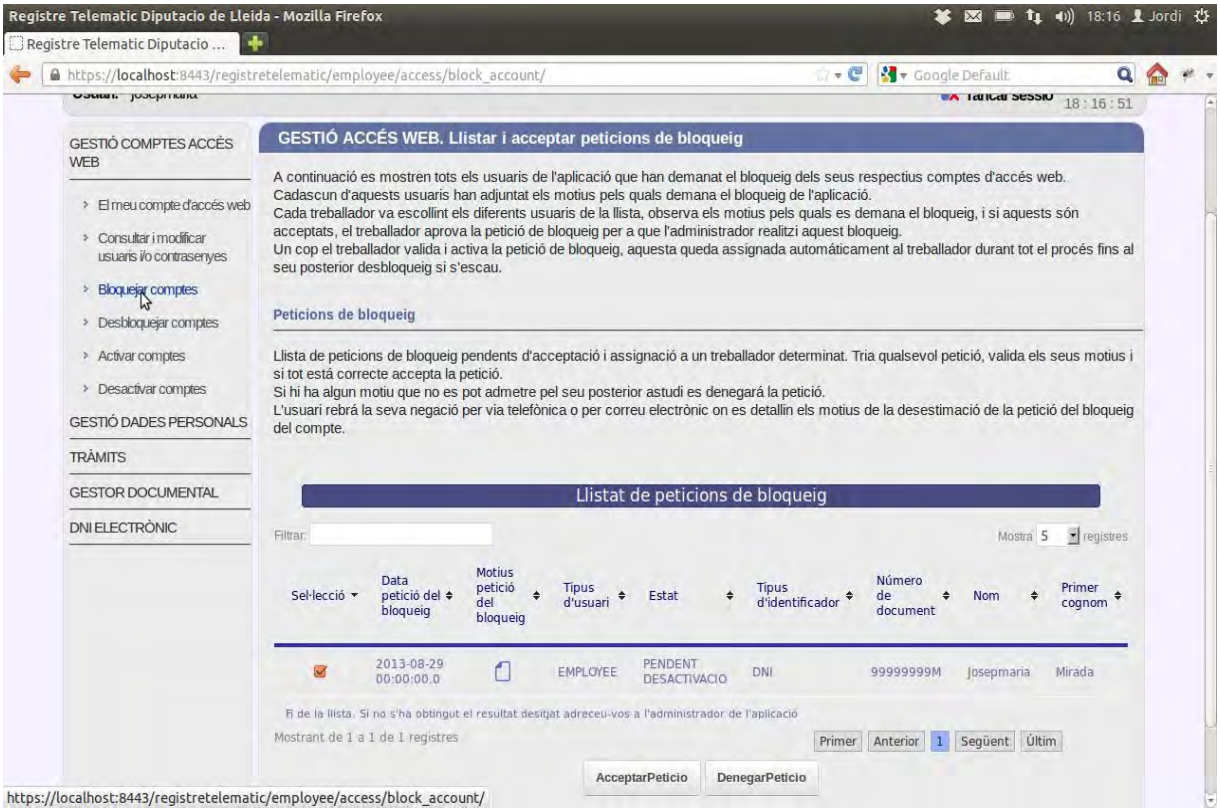


Il·lustració 63: Llistat de resultat del cercador de comptes web

Un cop la taula contingui resultats, l'empleat pot seleccionar qualsevol dels usuaris, i un cop fet, prémer el botó **"Consultar/Modificar"**. Mitjançant aquests passos, s'obrirà la pàgina de modificació del compte d'usuari seleccionat, on les dades podran ser alterades. Anàlogament a la modificació del compte del propi empleat que ha iniciat sessió, si les dades introduïdes són incorrectes, es mostrarà un missatge d'error a la vora de la dada errònia. Si les dades són correctes, es mostrarà una pantalla informant de modificació correcta de les dades.

5.2.2.3 Bloquejar comptes d'usuaris

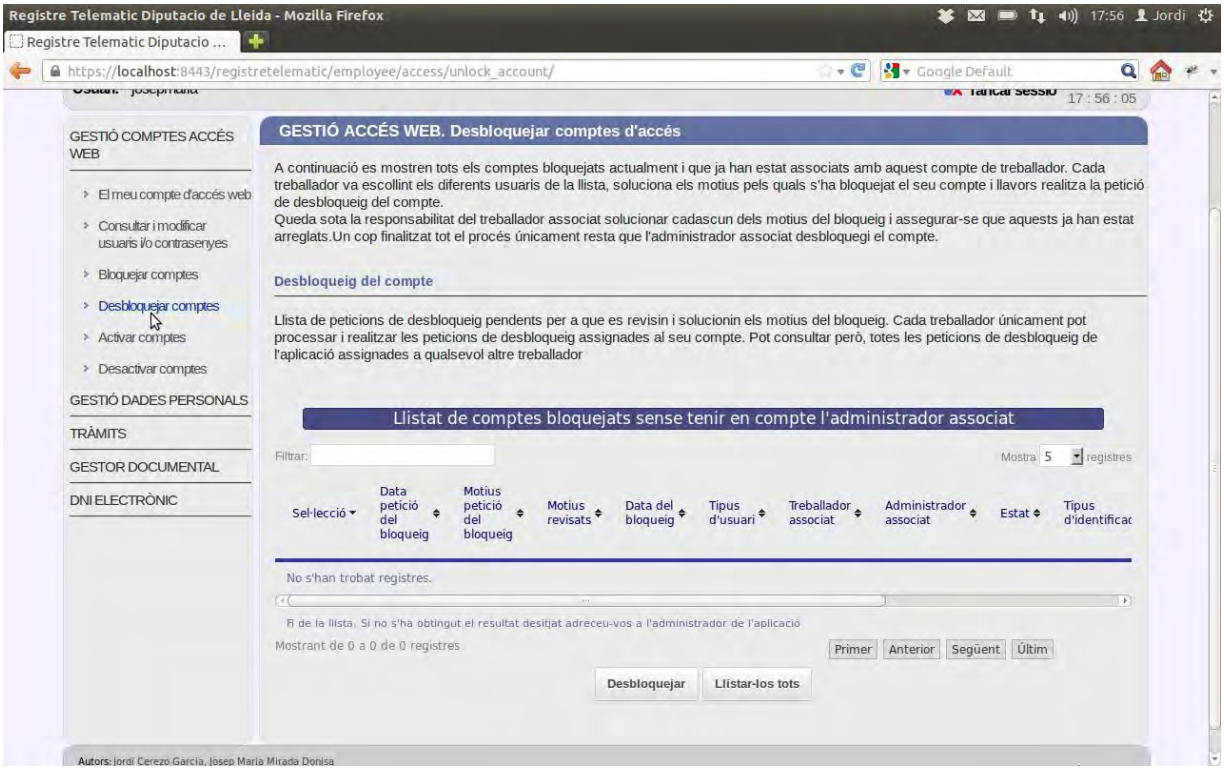
La següent entrada del menú de comptes d'usuaris és la etiquetada com a **"Bloquejar comptes d'usuari"**. En prémer aquest enllaç, l'empleat serà adreçat a una pàgina on es llisten totes les peticions de bloqueig de comptes realitzades per ciutadans que hi ha pendents a la base de dades de l'aplicació a la taula de la part inferior (Il·lustració 64). L'empleat pot comprovar els motius adduïts per demanar el bloqueig del compte, i si els troba coherents, pot marcar la petició de bloqueig referida, i acceptar-la prement el botó **"Acceptar Petició"**. També pot denegar aquest bloqueig si els motius no li semblen convincents prement el botó **"Denegar Petició"**. En qualsevol cas, la resolució de la petició de bloqueig haurà de ser notificada a l'usuari via telefònica, o bé a través de correu electrònic. El compte d'usuari bloquejat o desbloquejat quedarà pendent de l'actuació d'un usuari **Administrador** de l'aplicació, que serà qui finalment doni el vist-i-plau al bloqueig o desbloqueig d'un compte.



Il·lustració 64: Bloquejar comptes d'usuari

5.2.2.4 Desbloquejar comptes d'usuaris

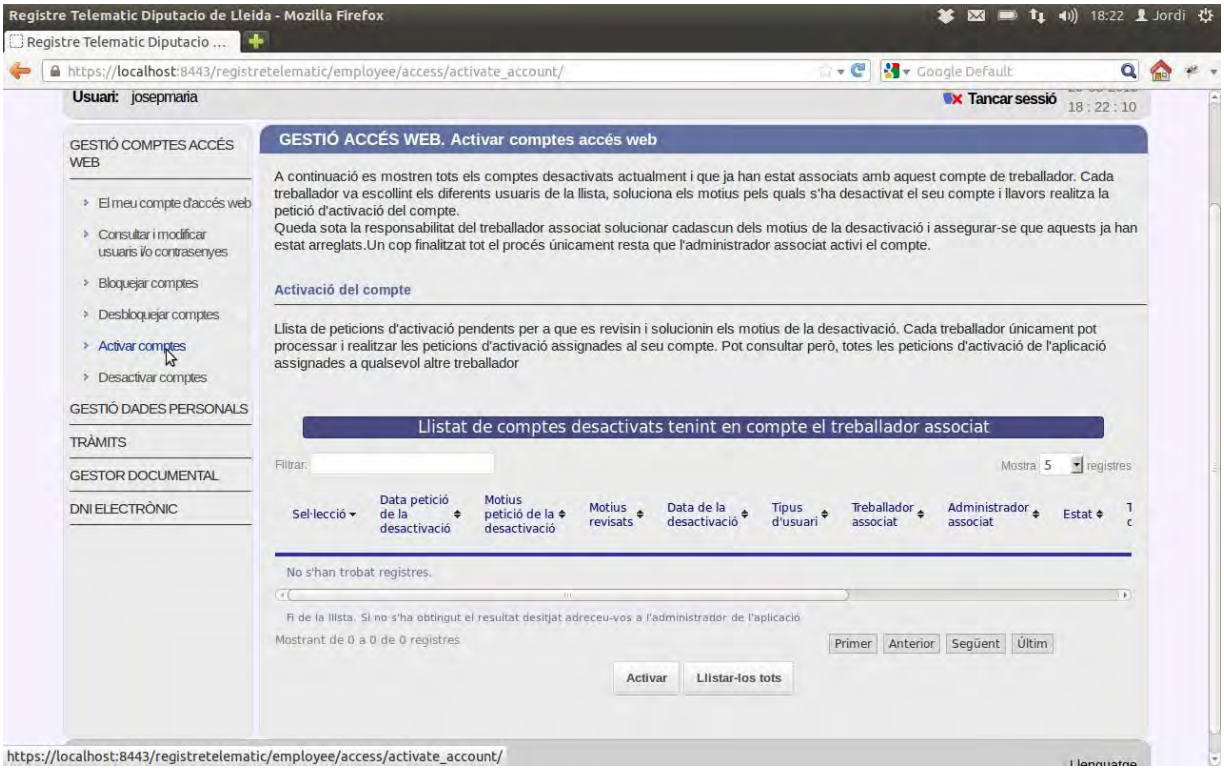
L'entrada del menú etiquetada com a **"Desbloquejar comptes d'usuari"**, adreçarà l'empleat a una pàgina on es llisten tots els comptes d'usuari bloquejats per ell que es troben a la base de dades de l'aplicació. Seran mostrats a la taula de la part inferior (Il·lustració 65). Si es vol desbloquejar un dels perfils i tornar-li la seva funcionalitat original, l'empleat l'ha de marcar a la taula, i ha de prémer el botó **"Desbloquejar"**. L'empleat només pot fer peticions de desbloqueig als comptes d'usuari de la web que ell mateix va bloquejar prèviament, i que seran els que es mostren per defecte a la taula d'aquesta pantalla. Existeix la possibilitat, però, de consultar tots els comptes bloquejats de l'aplicació, encara que estiguin assignats a altres treballadors. Per fer-ho, s'ha de prémer el botó **"Llistar-los tots"** de la part inferior de la pantalla. Per tornar a mostrar només els comptes propis del treballador que ha iniciat sessió, s'ha de prémer el mateix botó, etiquetat ara com a **"Llistar els propis"**. El compte d'usuari desbloquejat quedarà pendent de l'actuació d'un usuari **Administrador** de l'aplicació, que serà qui finalment doni el vist-i-plau al desbloqueig d'un compte.



Il·lustració 65: Desbloquejar comptes d'usuari

5.2.2.5 Activar comptes d'usuaris

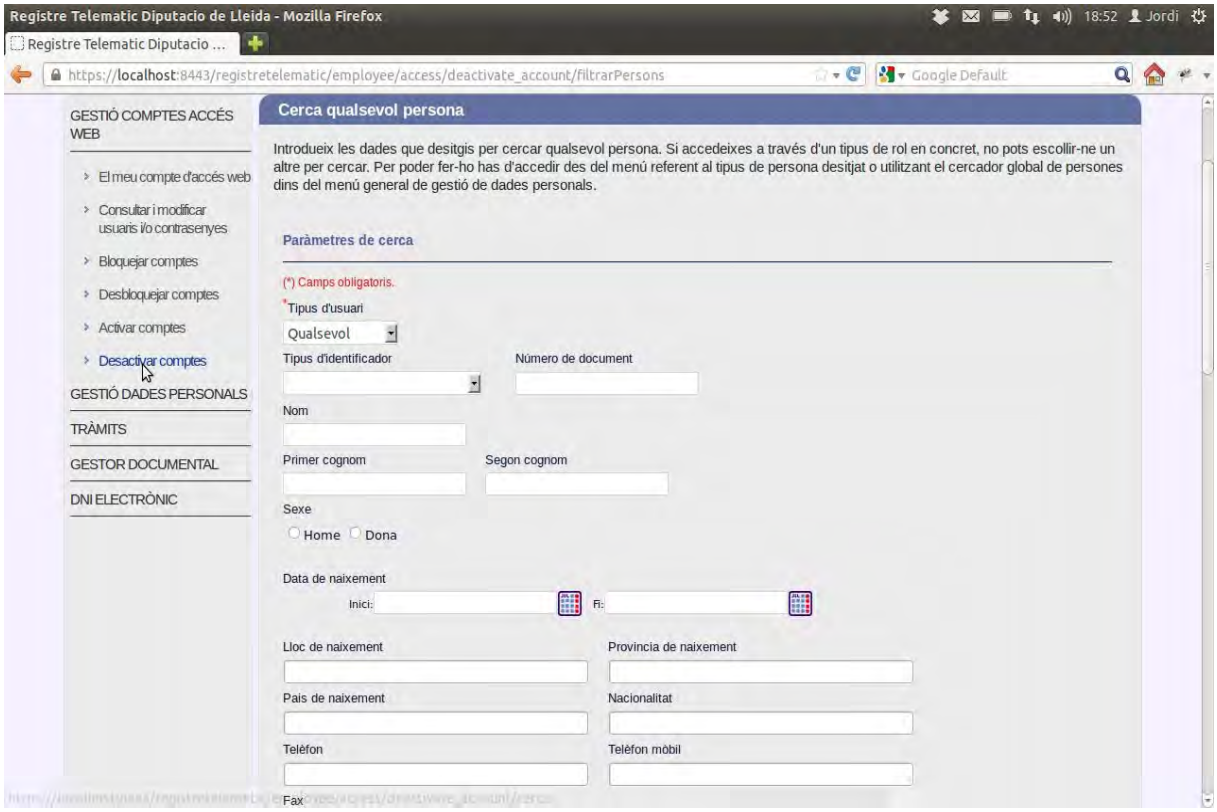
La següent entrada del menú de comptes d'usuaris és la etiquetada com a **"Activar comptes d'usuari"**. En prémer aquest enllaç, l'empleat serà adreçat a una pàgina on es llisten els comptes d'usuari que han estat desactivats per ell a la base de dades de l'aplicació, mitjançant una taula que es troba a la part inferior de la pàgina i que disposa de diverses funcionalitats pròpies (Il·lustració 66). A la part superior esquerra de la taula hi ha una caixa de text mitjançant la qual es poden filtrar els resultats, amb a finalitat d'afinar encara més la cerca. A la part superior dreta es pot introduir el número de registres que es volen mostrar a cada pàgina de la taula. A la part inferior dreta hi ha una sèrie de botons que permeten la navegació a través dels registres de la taula, portant a l'usuari de forma directa a la primera pàgina, la pàgina anterior, la pàgina següent, la pàgina final, i qualsevol d'elles de manera directa, mitjançant el seu número. L'empleat pot comprovar els motius adduïts per demanar la reactivació d'un compte prèviament desactivat, i si els troba coherents, pot marcar el checkbox de la petició d'activació referida, i prémer el botó **"Activar"**. L'empleat només pot reactivar els comptes d'usuari que van ser desactivats per ell, i que seran els que es mostren per defecte a la taula d'aquesta pantalla. Això és degut a que aquest empleat és qui coneix els motius de la petició de desactivació, i per tant, ha de ser ell qui valori si aquests motius han cessat. Existeix la possibilitat, però, de consultar tots els comptes desactivats de l'aplicació, encara que estiguin assignats a altres treballadors. Per fer-ho, s'ha de prémer el botó **"Llistar-los tots"** de la part inferior de la pantalla. Per tornar a mostrar només els comptes assignats al treballador que ha iniciat sessió, s'ha de prémer el mateix botó, etiquetat ara com a **"Llistar els propis"**. En qualsevol cas, la resolució de la reactivació del compte quedarà pendent de revisió per part d'un usuari **Administrador** de l'aplicació, que serà qui doni el vist-i-plau final a la reactivació del compte.



Il·lustració 66: Activació de comptes

5.2.2.6 Desactivar comptes d'usuari

El darrer botó del menú de **"Gestió de comptes d'accés web"** ens adreça directament a un cercador de persones (Il·lustració 68) per a la desactivació del seu comptes d'usuari web associat.



Il·lustració 67: Cercador de persones per a la desactivació de comptes d'usuari

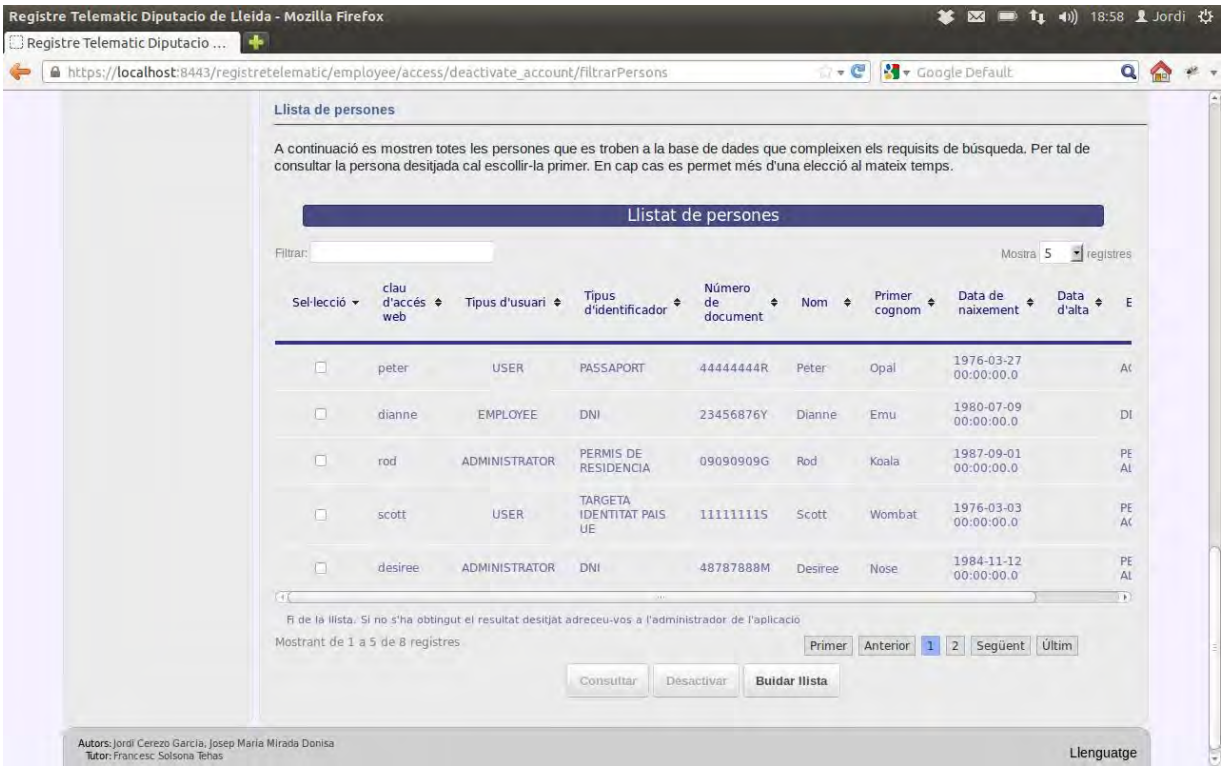
Aquesta pàgina permet realitzar una cerca de persones, filtrant els resultats per tots aquells paràmetres que es troben en pantalla, i mostrant els resultats a la taula de la part inferior:

- **Tipus d'usuari**: permet escollir el tipus d'usuari a cercar, administrador, empleat o usuari. Si es deixa en “Qualsevol”, es cercarà per tots els tipus d'usuari.
- **Tipus d'identificador/Número de document**: permet triar el tipus de document mitjançant el qual la persona es va identificar per donar-se d'alta a l'aplicació, i el número d'aquest document.
- **Nom i cognoms**: permet cercar segons el nom i cognoms de l'usuari. La cerca es realitza per comparació de cadenes de text, de tal manera que, si només coneixem una part del nom, podem escriure només aquella part, i l'aplicació cercarà els usuaris que continguin aquella part.
- **Sexe**: segons si és home o dona. Si no es marca un dels dos, aquest paràmetre no es tindrà en compte (es mostraran els usuaris d'ambdós sexes).
- **Data de naixement**: l'aplicació permet acotar la data de naixement a dos dates concretes. Si no s'emplenen aquests camps, el paràmetre no es tindrà en compte. Si només es plena la data d'inicial, es mostraran les persones amb data de naixement posterior a la introduïda. Si només es plena la data final, es mostraran les persones amb data de naixement anterior a la introduïda.
- **Lloc de naixement**: permet buscar persones nascudes a una localitat concreta.
- **Província de naixement**: permet buscar persones nascudes a una província concreta.

- **País de naixement**: permet buscar persones nascudes a un país concret.
- **Nacionalitat**: permet buscar persones d'una nacionalitat concreta.
- **Telèfon**: permet buscar persones segons el seu telèfon.
- **Telèfon mòbil**: permet buscar persones segons el seu telèfon mòbil.
- **Fax**: permet buscar persones segons el seu fax.
- **Clau d'accés web**: permet cercar segons la seva contrasenya.
- **Estat**: permet cercar segons l'estat del compte a la base de dades.
- **Dates d'alta, baixa i modificació**: Aquestes dates corresponen als moments en que els registres de les persones que es troben a la base de dades han estat introduïts, modificats per darrera vegada, i donats de baixa, si és el cas. Si només es plena la data d'inicial, es mostraran les persones amb data d'alta, baixa o modificació posterior a la introduïda. Si només es plena la data final, es mostraran les persones amb data d'alta, baixa i modificació anterior a la introduïda.

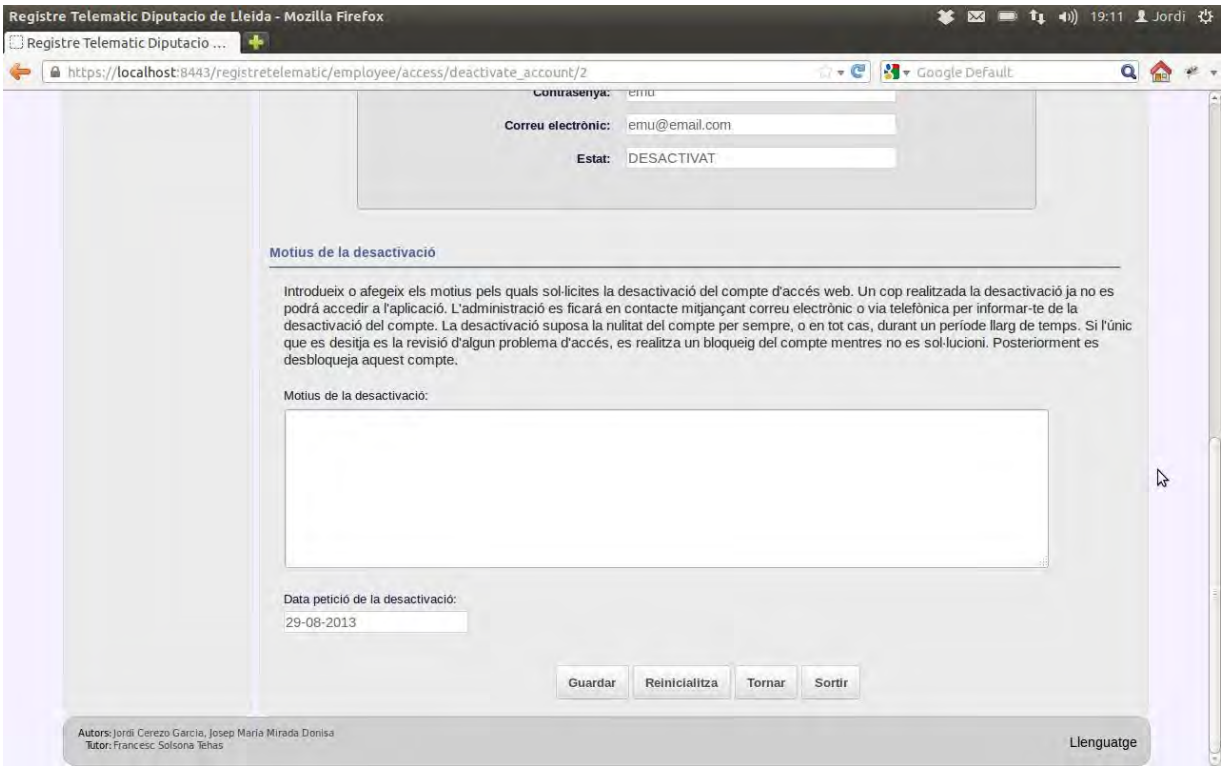
És possible també realitzar una ordenació dels resultats segons qualsevol dels paràmetres presents al desplegable "Ordenat per:", i disposar-los de manera ascendent o descendent. Per realitzar la cerca, s'ha de prémer el botó **"Cercar"**. El botó **"Reinicialitza"** restaura tots els camps del cercador al seu estat per defecte. El botó **"Buidar llista"** permet buidar la llista de la taula inferior, corresponent a la darrera cerca realitzada. El botó **"Sortir"** ens porta directament a la pantalla inicial de l'aplicació.

La llista de la part inferior de la pantalla contindrà, com s'ha esmentat anteriorment, els resultats de la la darrera cerca realitzada (Il·lustració 68).



Il·lustració 68: Llistat de persones per a la desactivació de comptes

Un cop la taula contingui resultats, l'empleat pot buidar els resultats de la taula prement el botó **“Buidar llista”**, o bé pot seleccionar qualsevol dels usuaris (la selecció serà sempre unitària, és a dir, no es poden seleccionar dos o més dels registres que apareixen a la taula). Si l'empleat prem el botó **“Consultar”**, s'obrirà la pàgina de consulta de les dades de la persona escollida. La desactivació es durà a terme prement el botó **“Desactivar”**, el qual ens portarà a una pàgina que ens mostra les dades de la persona (Il·lustració 69), i ens permet desactivar el compte mitjançant el botó **“Guardar”**, introduint els motius corresponents pels quals es realitza aquesta desactivació. Si la desactivació és correcta, es mostrarà una pantalla informant de l'èxit de l'operació.



Il·lustració 69: Confirmació de desactivació

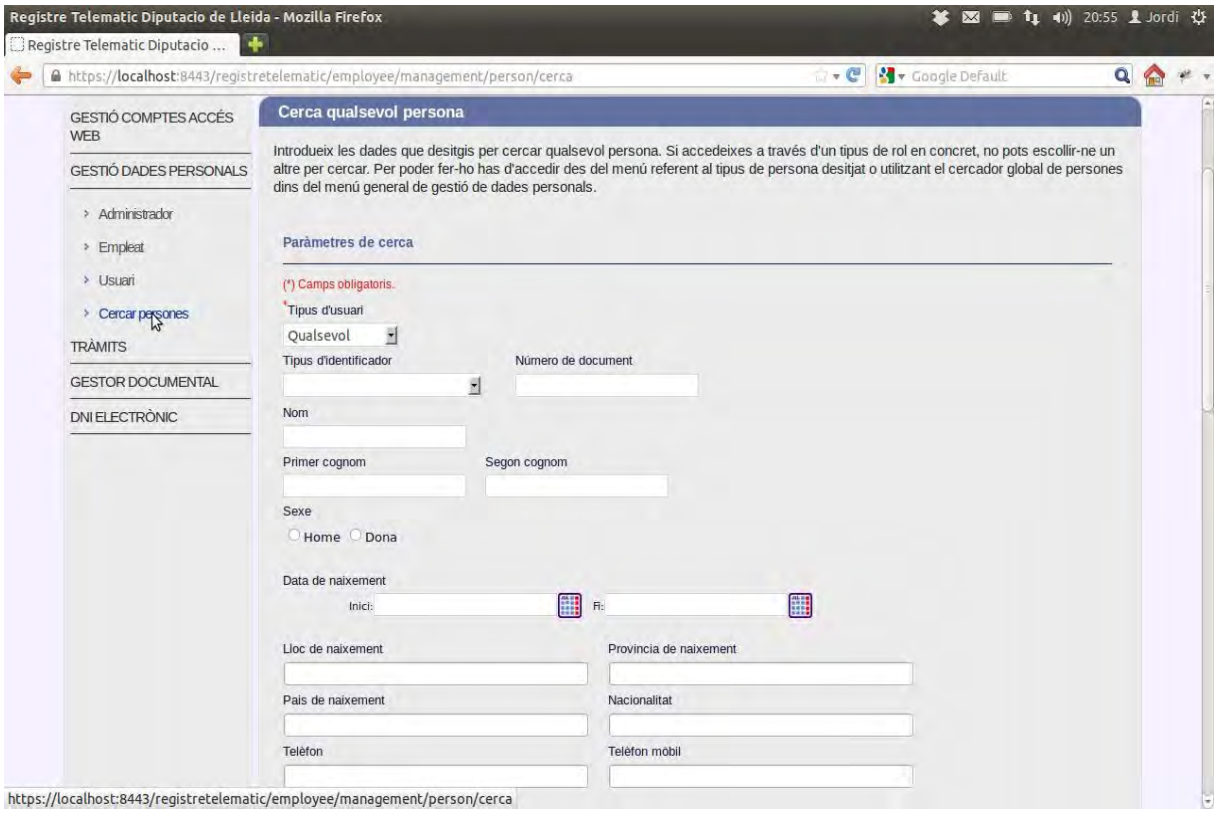
5.2.3 Gestió de dades personals

Aquesta segona entrada del menú principal permetrà a l'empleat realitzar la gestió i manteniment de les dades personals dels usuaris presents a la base de dades. Primerament comentarem l'últim dels botons continguts en aquesta branca del menú, el **“Cercador de persones”**. Es farà d'aquesta forma, degut a que aquest mateix cercador serà emprat, amb petites modificacions, a la consulta i modificació de les dades dels usuaris.

També s'ha de matisar que, tot i que al menú s'ha realitzat una divisió dels tipus d'usuari presents a l'aplicació, en aquest manual d'instruccions només comentarem les tasques associades a ells, és a dir, “Alta”, “Consulta” i “Modificació”. Es farà d'aquesta manera per que les tasques que es poden realitzar a cada tipus d'usuari són les mateixes, i aquesta divisió només respon a un intent de donar més claredat a les tasques de l'empleat. Per aquest motiu, les diferents tasques es tractaran de manera global, sobreentenent que s'està gestionant un usuari de tipus específic, depenent del tipus d'usuari escollit per l'empleat.

5.2.3.1 Cercador de persones

Com s'acaba de comentar, el primer botó que tractarem en aquest apartat és el que està etiquetat com a **“Cercar persones”**. Aquest cercador ens permetrà buscar les persones emmagatzemades a la base de dades de l'aplicació (Il·lustració 70) permetent realitzar una cerca de persones, filtrant els resultats per tots els paràmetres que es troben en pantalla, i mostrant els resultats a la taula de la part inferior:



Il·lustració 70: Cercador d'usuaris global

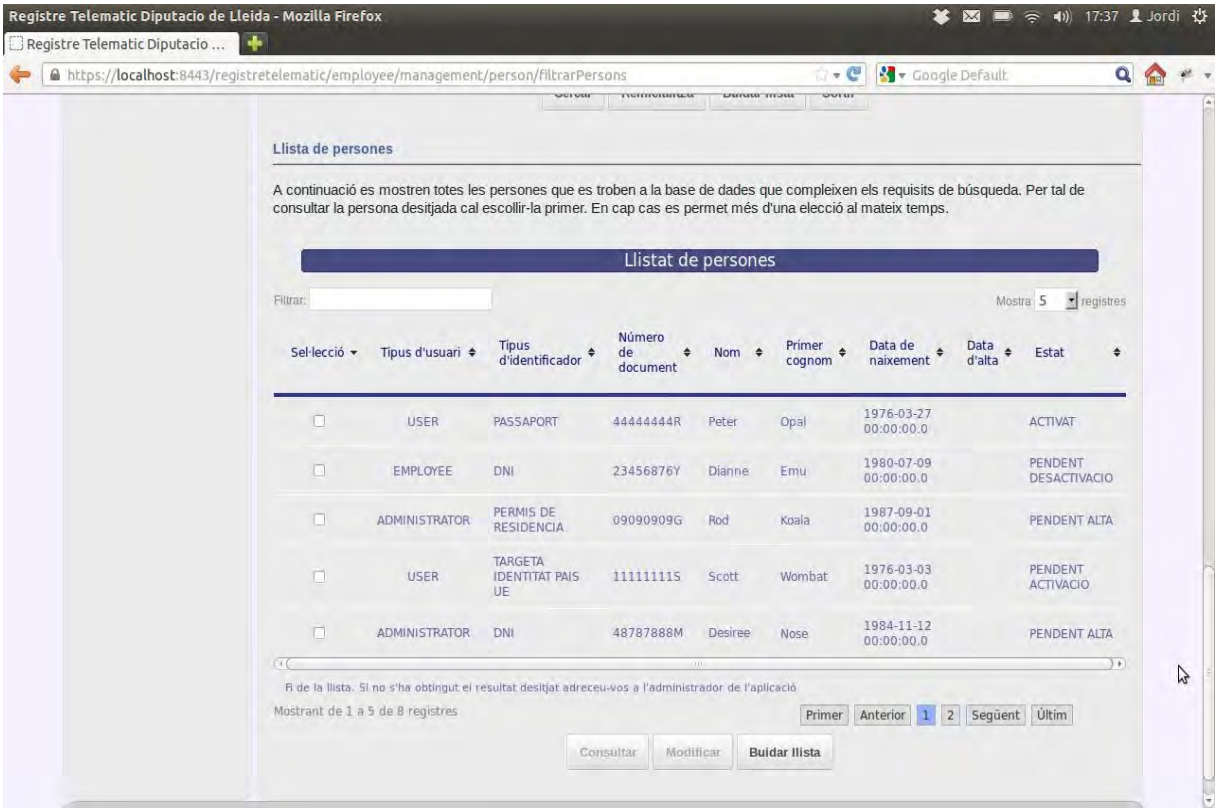
- **Tipus d'usuari**: permet seleccionar el tipus d'usuari que volem buscar. Els possibles valors són “Administrador”, “Empleat” o “Usuari”. Existeix la possibilitat de cerca entre tots els tipus d'usuari marcant la opció **“Qualsevol”**.
- **Tipus d'identificador/Número de document**: permet triar el tipus de document mitjançant el qual la persona es va identificar per donar-se d'alta a l'aplicació, i el número d'aquest document.
- **Nom i cognoms**: permet cercar segons el nom i cognoms de l'usuari. La cerca es realitza per comparació de cadenes de text, de tal manera que, si només coneixem una part del nom, podem escriure només aquella part, i l'aplicació cercarà els usuaris que continguin aquella part.
- **Sexe**: segons si és home o dona. Si no es marca un dels dos, aquest paràmetre no es tindrà en compte (es mostraran els usuaris d'ambdós sexes).
- **Data de naixement**: l'aplicació permet acotar la data de naixement a dos dates concretes. Si no s'emplenen aquests camps, el paràmetre no es tindrà en compte. Si només es plena la data d'inicial, es mostraran les persones amb data de naixement posterior a la introduïda. Si

només es plena la data final, es mostraran les persones amb data de naixement anterior a la introduïda.

- **Lloc de naixement**: permet buscar persones nascudes a una localitat concreta.
- **Província de naixement**: permet buscar persones nascudes a una província concreta.
- **País de naixement**: permet buscar persones nascudes a un país concret.
- **Nacionalitat**: permet buscar persones d'una nacionalitat concreta.
- **Telèfon**: permet buscar persones segons el seu telèfon.
- **Telèfon mòbil**: permet buscar persones segons el seu telèfon mòbil.
- **Fax**: permet buscar persones segons el seu fax.
- **Clau d'accés web**: permet cercar segons la seva contrasenya.
- **Estat**: permet cercar segons l'estat del compte a la base de dades.
- **Dates d'alta, baixa i modificació**: Aquestes dates corresponen als moments en que els registres de les persones que es troben a la base de dades han estat introduïts, modificats per darrera vegada, i donats de baixa, si és el cas. Si només es plena la data d'inicial, es mostraran les persones amb data d'alta, baixa o modificació posterior a la introduïda. Si només es plena la data final, es mostraran les persones amb data d'alta, baixa i modificació anterior a la introduïda.

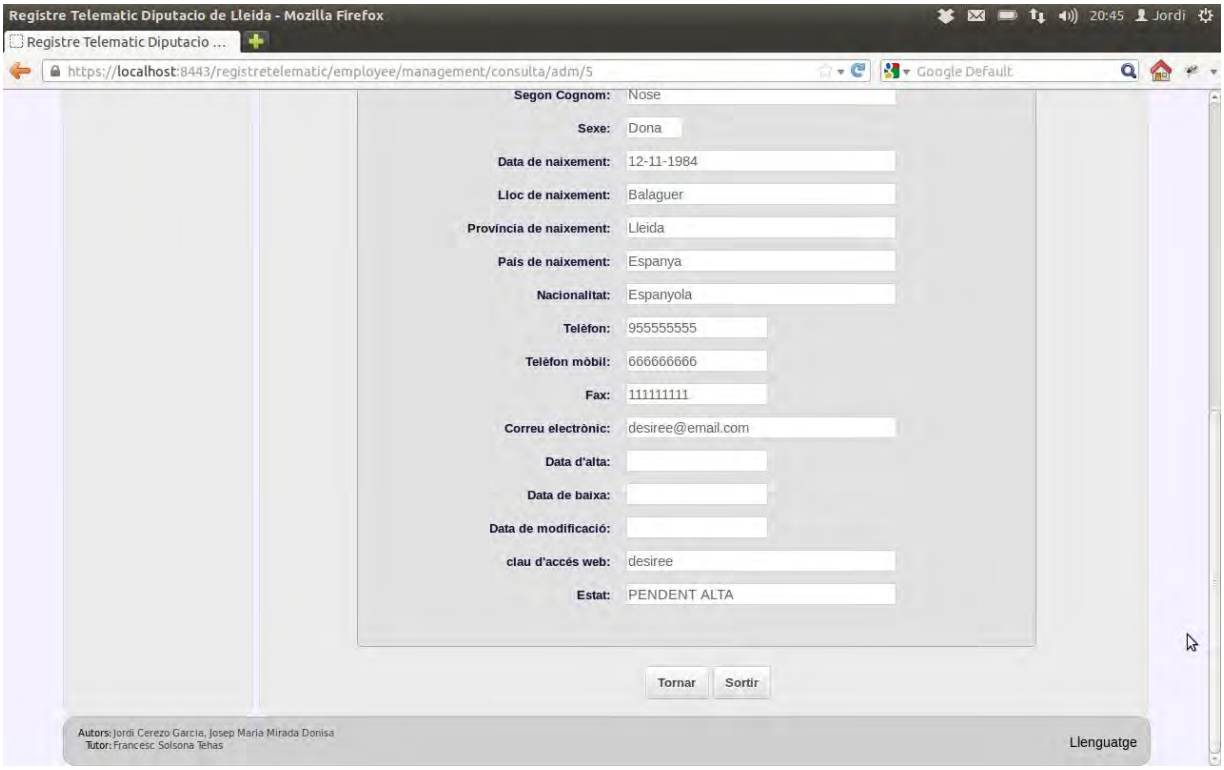
És possible també realitzar una ordenació dels resultats segons qualsevol dels paràmetres presents al desplegable “Ordenat per:”, i disposar-los de manera ascendent o descendent. Per realitzar la cerca, s'ha de prémer el botó **“Cercar”**. El botó **“Reinicialitza”** restaura tots els camps del cercador al seu estat per defecte. El botó **“Buidar llista”** permet buidar la llista de la taula inferior, corresponent a la darrera cerca realitzada. El botó **“Sortir”** ens porta directament a la pantalla inicial de l'aplicació.

La llista de la part inferior de la pantalla contindrà, com s'ha esmentat anteriorment, els resultats de la la darrera cerca realitzada (Il·lustració 71).

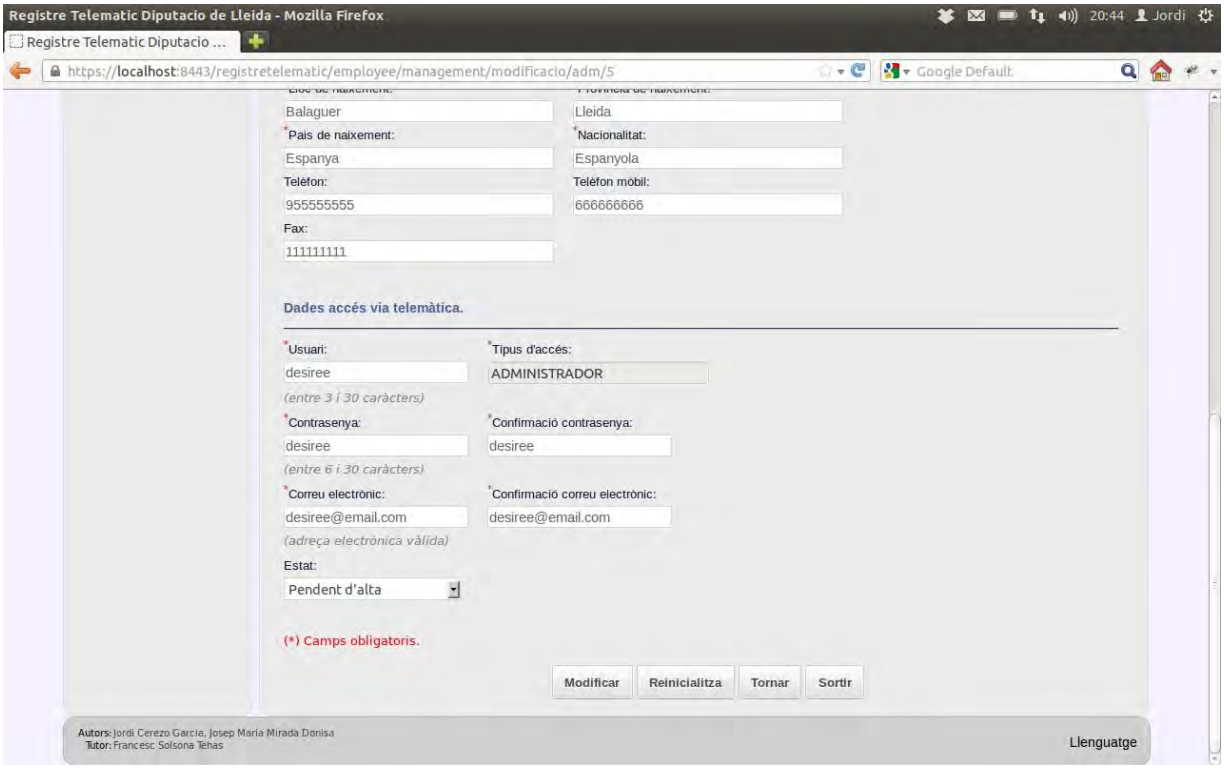


Il·lustració 71: Llistat de resultats de la cerca d'usuaris

Un cop la taula contingui resultats, l'empleat pot marcar qualsevol dels usuaris, i un cop fet, prémer el botó **"Consultar"** o bé **"Modificar"** (Il·lustració 71), acció que ens portarà directament al formulari de consulta (Il·lustració 72) mostrant en pantalla les dades referents a l'usuari seleccionat. En aquesta pantalla podem sortir de la pàgina inicial prement el botó **"Sortir"**, o bé retornar al cercador de persones prement **"Tornar"**. El formulari de modificació (Il·lustració 73) permet alterar les dades corresponents a l'usuari seleccionat. Els camps obligatoris estan marcats amb un asterisc vermell. Per guardar les modificacions, s'ha de prémer el botó **"Guardar"**. Si les dades introduïdes són incorrectes o incompletes, es mostraran els missatges d'error corresponents a la vora dels camps corresponents del formulari. Si són correctes, es mostrarà un missatge informant de l'èxit de l'operació.



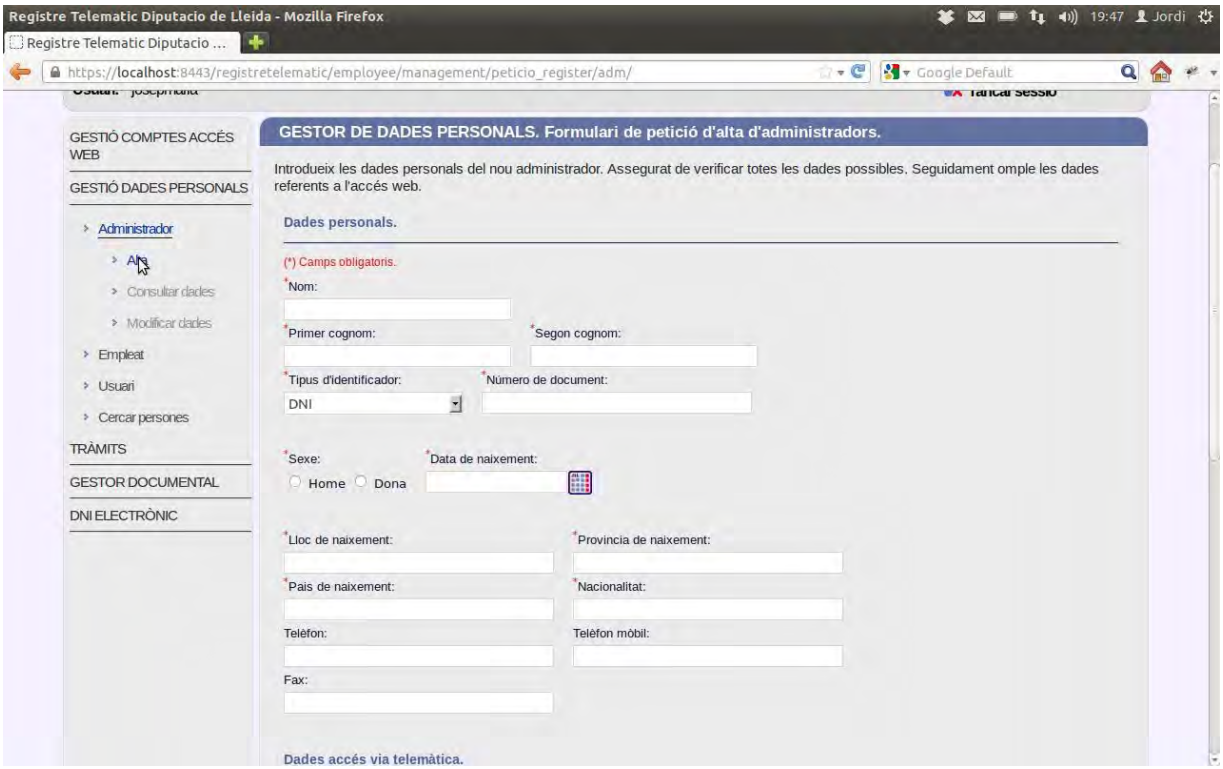
Il·lustració 72: Consulta d'usuari



Il·lustració 73: Modificació d'usuari

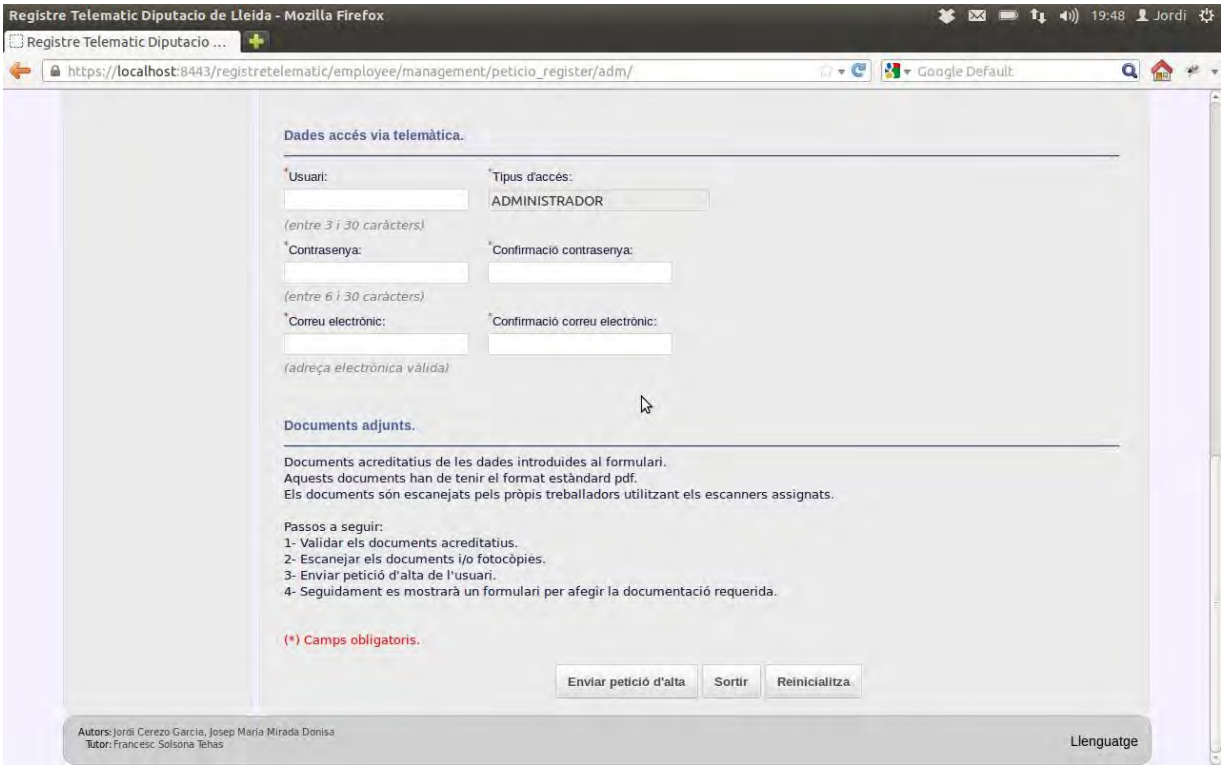
5.2.3.2 Alta d'usuari

Aquest botó permet a l'empleat dóna d'alta un nou usuari, ja sigui “Administrador, “Empleat” o “Usuari” (Il·lustració 74). Es mostrarà en pantalla un formulari en el qual s'han d'introduir les dades del nou usuari. Els camps marcats amb un asterisc de color vermell indiquen camps obligatoris. En cas que es deixin buits o bé les dades no es corresponguin al tipus esperat, apareixerà un missatge d'error a la vora de la caixa de text que conté les dades incorrectes. Un cop les dades siguin correctes, en prémer el botó **“Enviar petició d'alta”** (Il·lustració 75) les dades s'emmagatzemaran a l'aplicació, i restaran pendents de l'acceptació del nou 'usuari per part d'un dels Administradors del programa. El botó **“Sortir”** anul·larà la petició d'alta i ens retornarà a la pàgina inicial de l'aplicació. El botó **“Reinicialitza”** tornarà tots els camps del formulari al seu estat inicial.



Il·lustració 74: Alta d'usuaris (en aquest cas un “Administrador”)

Quan aquestes dades siguin acceptades, l'usuari passarà a ser vàlid a l'aplicació, i es podran realitzar les tasques associades disponibles a l'aplicació, accedint amb el nom d'usuari i contrasenya corresponents.



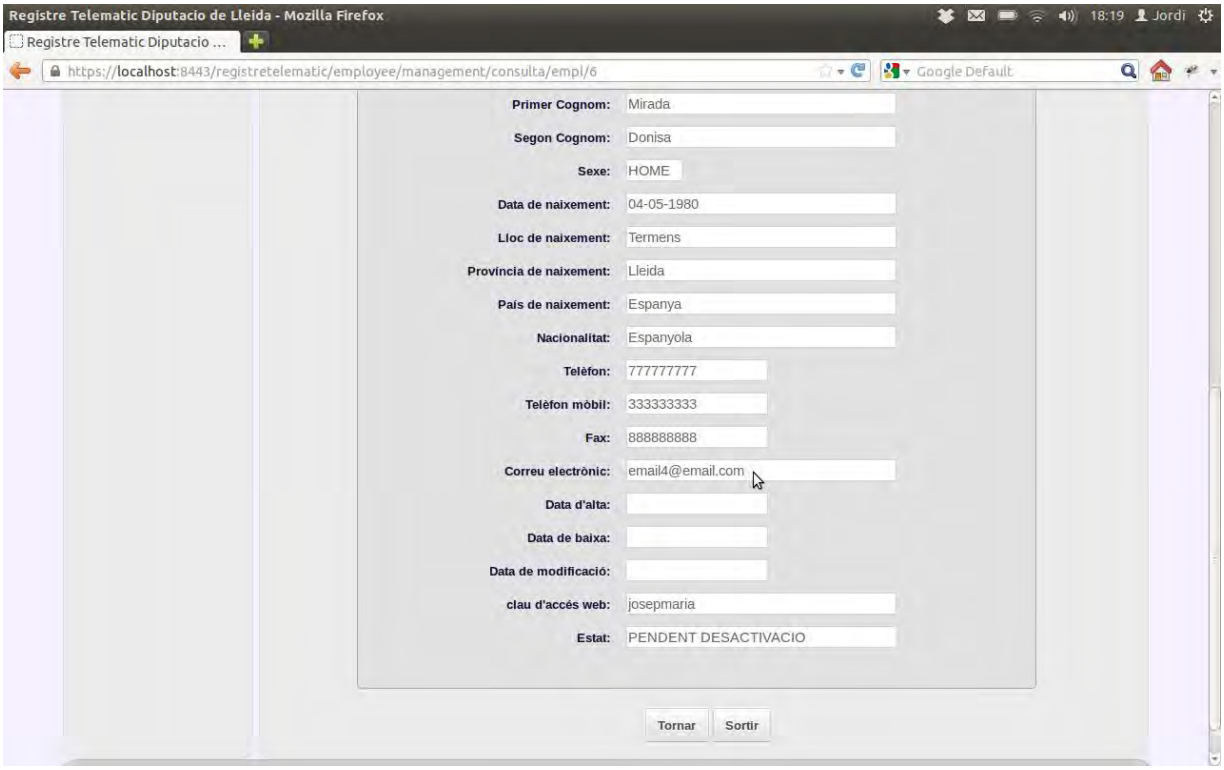
Il·lustració 75: Alta d'usuari (en aquest cas un "Administrador"), detall botons

5.2.3.3 Consulta d'usuari

El botó de **"Consulta"** portarà l'empleat directament al cercador de persones (5.2.3.1 Cercador de persones). La única diferència amb el cercador de persones global, prèviament comentat, serà que el camp "Tipus d'usuari" apareixerà deshabilitat, i contindrà el tipus d'usuari que s'ha escollit per consultar, "Administrador", "Empleat" o "Usuari".

Per realitzar la cerca, l'empleat ha de completar els diferents camps que acotaran els resultats. Un cop premi el botó **"Cercar"**, els resultats seran mostrats a la taula inferior. Per realitzar la consulta, l'empleat ha de seleccionar un dels usuaris llistats, i prémer el botó inferior **"Consultar"**. Una nova finestra apareixerà en pantalla mostrant les dades corresponents a l'usuari marcat (Il·lustració 76).

Les dades d'aquest formulari no poden ser alterades, només consultades (si es volen modificar, s'ha de consultar l'apartat 5.2.3.4 Modificació usuari). A la part inferior d'aquesta pantalla trobem dos botons. **"Sortir"** ens portarà directament a la pantalla inicial de l'aplicació. **"Tornar"** ens retornarà al cercador de persones, mantenint les opcions de la darrera cerca realitzada.



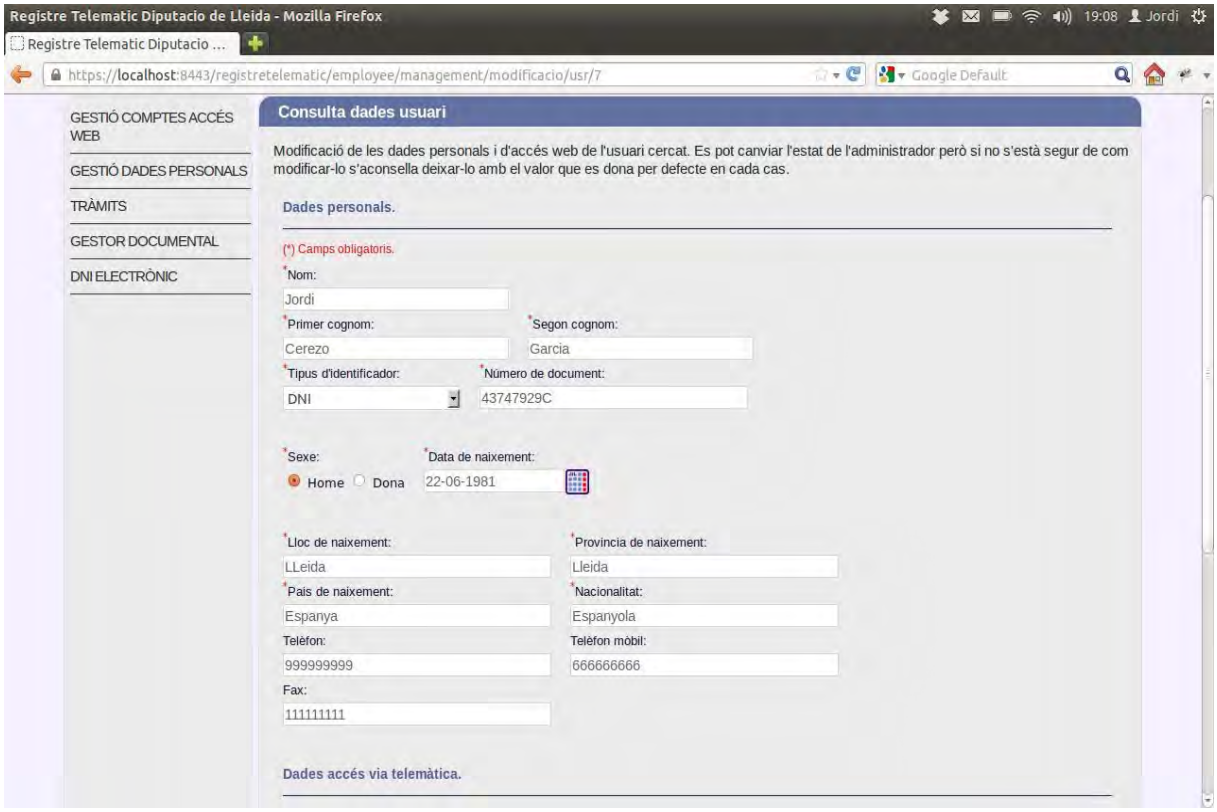
Il·lustració 76: Consulta d'usuari (en aquest cas un "Empleat")

5.2.3.4 Modificació usuari

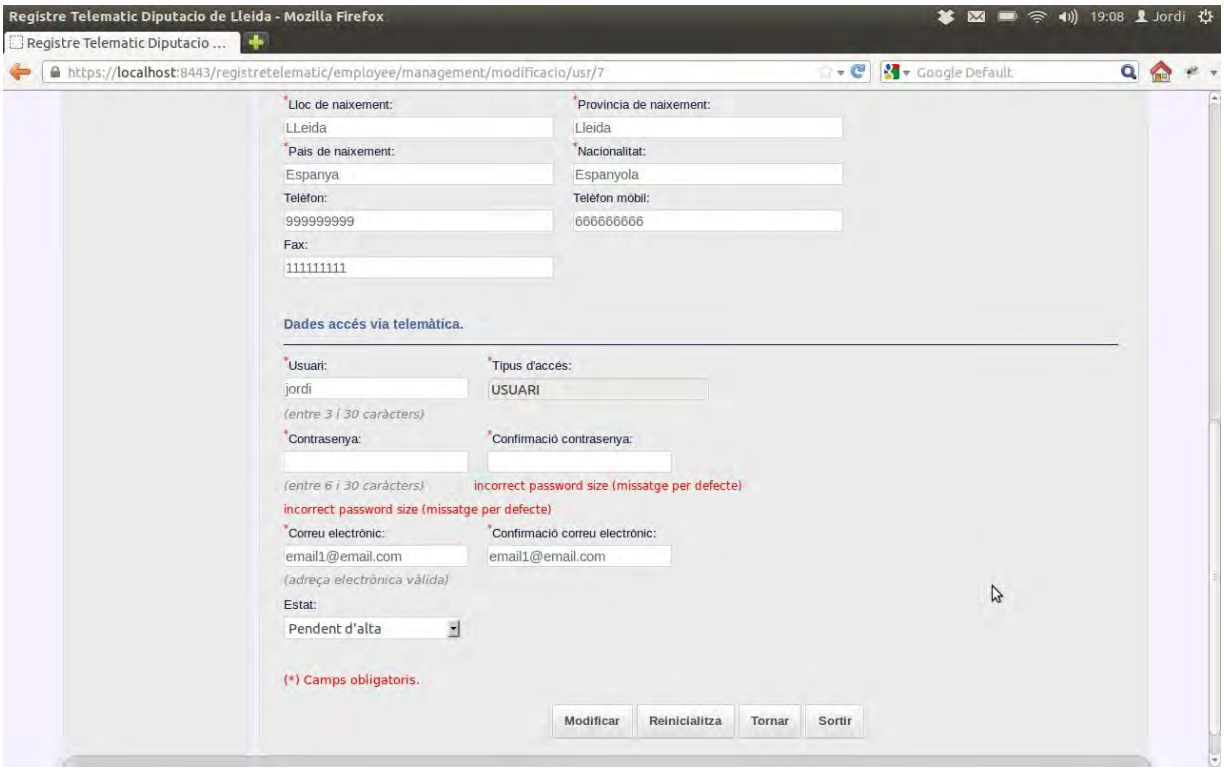
El botó de **“Modificació”** portarà l'empleat directament al cercador de persones (5.2.3.1 Cercador de persones). La única diferència amb el cercador de persones global, prèviament comentat, serà que el camp “Tipus d'usuari” apareixerà deshabilitat, i contindrà el tipus d'usuari que s'ha escollit per realitzar la modificació, “Administrador”, “Empleat” o “Usuari”.

Per realitzar la cerca, l'empleat ha de completar els diferents camps que acotaran els resultats. Un cop premi el botó **“Cercar”**, els resultats seran mostrats a la taula inferior. Per realitzar la modificació, l'empleat ha de seleccionar un dels usuaris llistats, i prémer el botó inferior **“Modificar”**. Una nova finestra apareixerà en pantalla mostrant les dades corresponents a l'usuari marcat (Il·lustració 77).

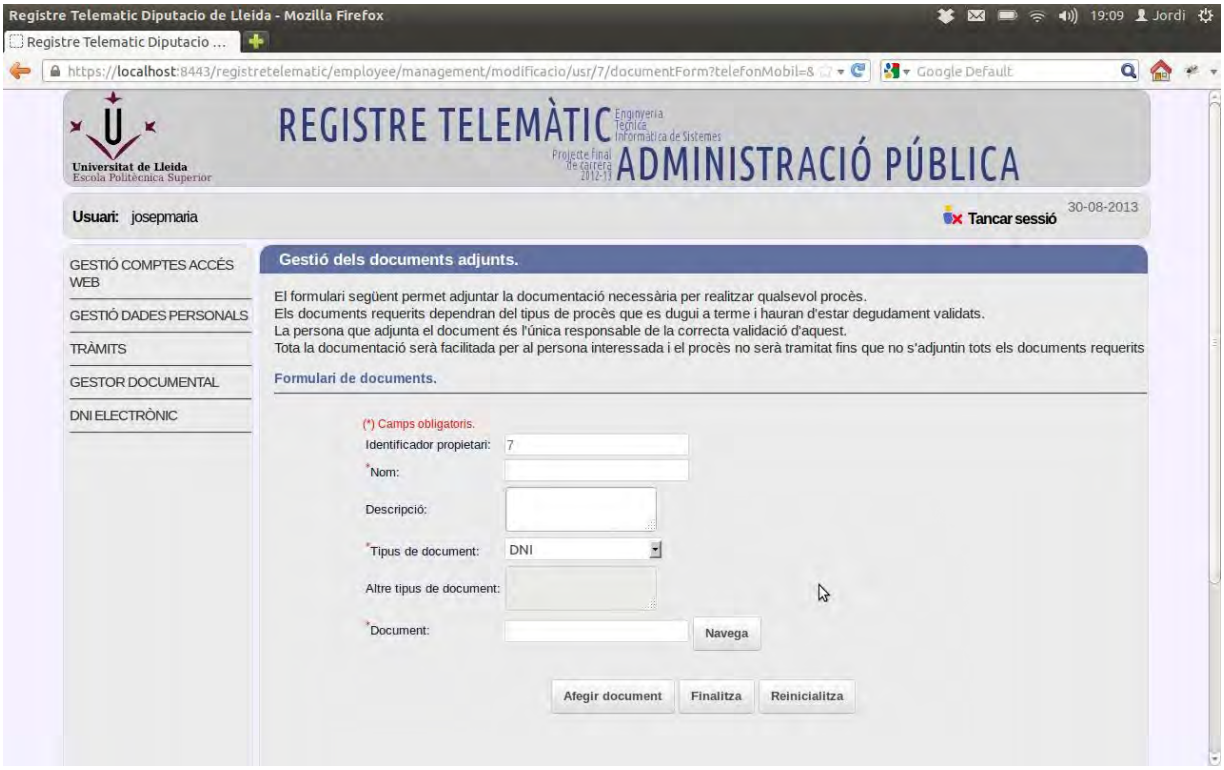
A la part inferior d'aquesta pantalla trobem diversos botons. **“Modificar”** servirà per confirmar la modificació de les dades. Si algun dels camps obligatoris queda buit, o bé el tipus de dades introduït no és correcte, apareixerà un missatge a la vora del camp informant de l'error (Il·lustració 78). Si les dades són correctes, l'empleat serà adreçat a la pantalla d'introducció de documents associats a l'usuari modificat, per tal d'emmagatzemar còpies dels documents que acrediten les dades proporcionades (Il·lustració 79) (la funcionalitat de **“Gestor documental”** serà tractada en profunditat més endavant en aquest manual). **“Reinicialitza”** posarà totes les dades de l'usuari en blanc. **“Tornar”** ens retornarà al cercador de persones, mantenint les opcions de la darrera cerca realitzada. “**Sortir”** ens portarà directament a la pantalla inicial de l'aplicació.



Il·lustració 77: Modificació d'usuari (en aquest cas, un "Usuari")



Il·lustració 78: Error a la modificació d'usuari



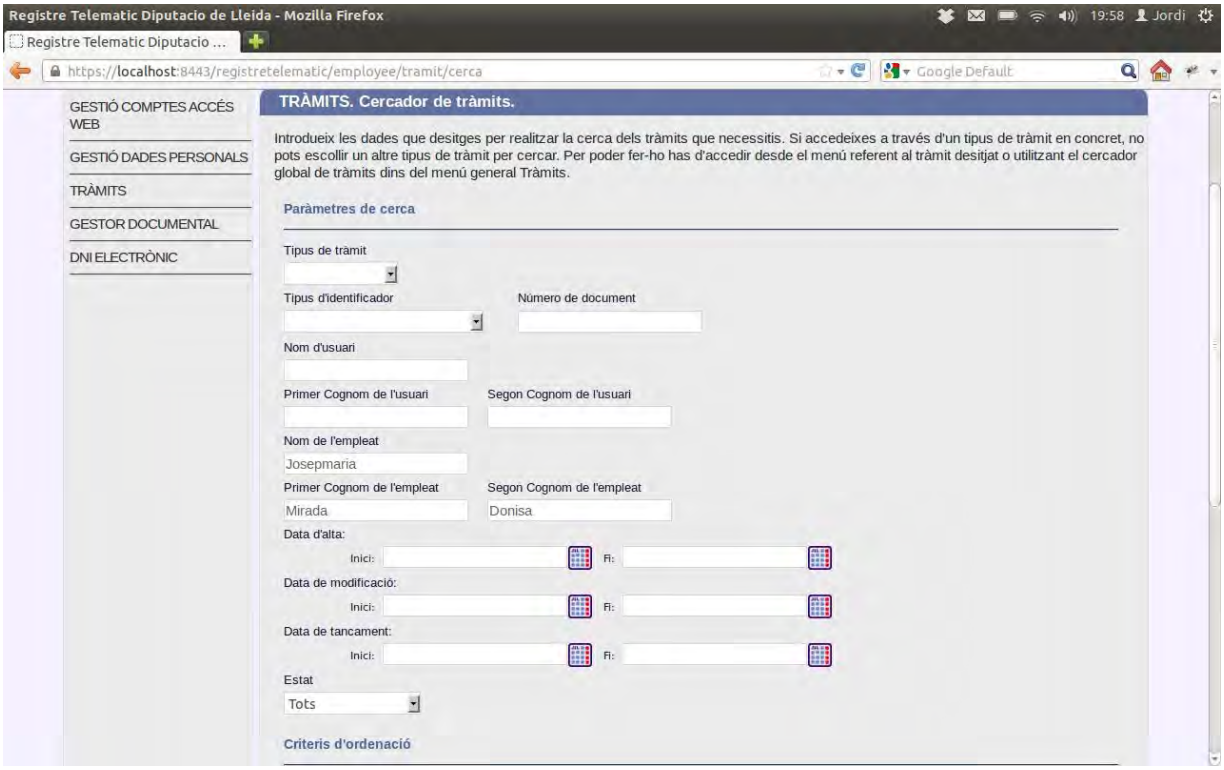
Il·lustració 79: Modificació d'usuari correcta

5.2.4 Tràmits

L'entrada de menú **"Tràmits"** porta l'empleat a tots els procediments relacionats amb els diferents tràmits que gestiona l'aplicació. En primer lloc, comentarem el botó que apareix en la posició inferior, **"Cercar qualsevol tràmit"**. Aquest cercador permetrà a l'empleat realitzar una cerca entre tots els tràmits presents a l'aplicació sense distinció de tipus. La resta de botons mostren les entrades de cadascun dels tipus de tràmits. L'empleat podrà fer cerques acotades només a un tipus de tràmits determinat segons la seva elecció, modificar les seves característiques, i donar d'alta i de baixa de la base de dades els tràmits que seleccionem. Passem a analitzar de forma més acurada cadascun dels botons.

5.2.4.1 Cercar qualsevol tràmit

El botó "Cercar tràmits" portarà l'empleat a una pàgina dedicada a la cerca de tràmits de tota mena a la base de dades (Il·lustració 80). Es pot considerar una cerca global de tràmits a la base de dades de l'aplicació, ja que no s'està tenint en compte quin tipus de tràmits és el que estem cercant. Aquestes seran les variables del cercador:



Il·lustració 80: Cercador de tràmits global

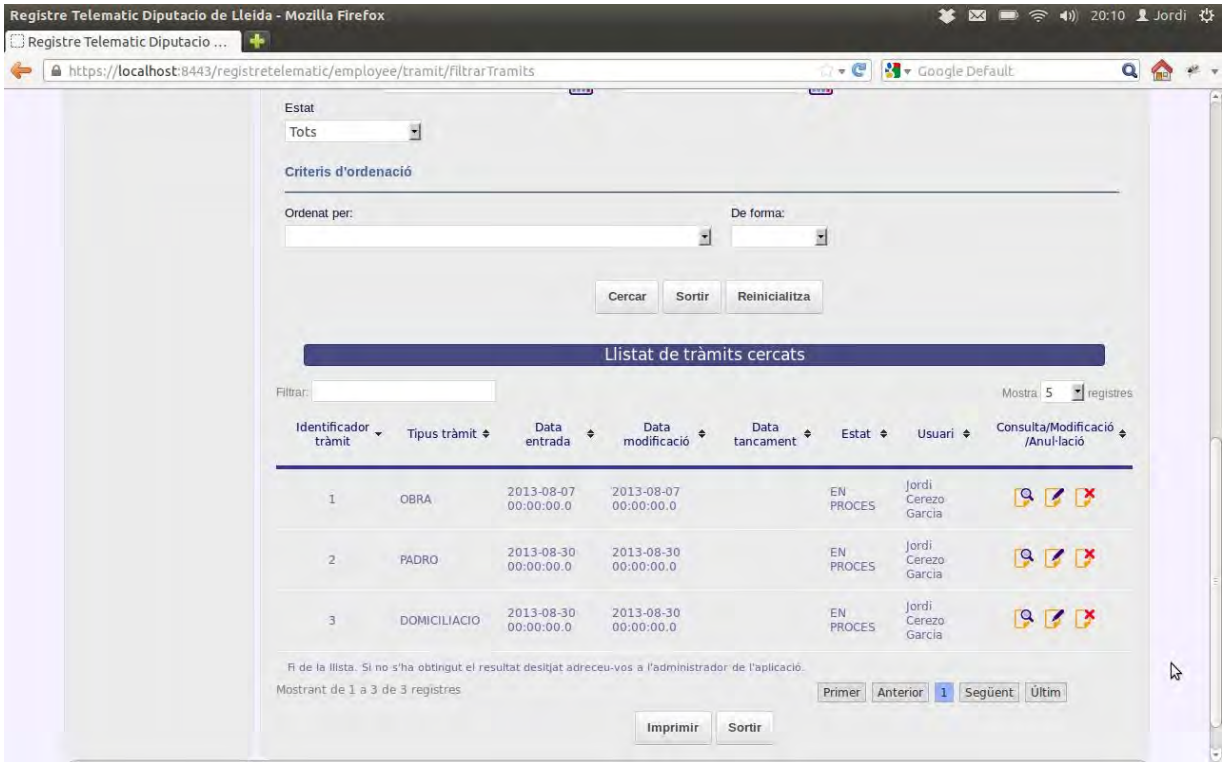
- **Tipus de tràmit**: a la part superior de la pàgina es troba un desplegable on es permet triar el tipus de tràmit que s'està cercant. Si no se'n tria cap, la cerca a la base de dades comprendrà tots els tipus de tràmits presents a l'aplicació.
- **Tipus identificador i número de document de l'usuari:** el tipus d'identificador i número de document, es refereixen al document identificador, que acredita la identitat de l'usuari propietari del tràmit. Per exemple, si l'usuari s'ha acreditat amb el Document Nacional d'Identitat, el tipus d'identificador serà “DNI”, i el número de document, serà el número de “DNI” de l'esmentat usuari. Si els camps es deixen en blanc, no es tindran en compte a l'hora de fer el filtre a la base de dades.
- **Nom, primer cognom i segon cognom de l'usuari**: aquest camps es refereixen al nom complet de l'usuari propietari del tràmit o tràmits cercats. El nom es cercarà comprovant si la cadena introduïda està continguda a les dades emmagatzemades a l'aplicació. Si els camps es deixen en blanc, no es tindran en compte a l'hora de fer el filtre a la base de dades.
- **Nom, primer cognom i segon cognom de l'empleat**: aquest camps es refereixen al nom complet de l'empleat que ha editat el tràmit o tràmits cercats. El nom es cercarà comprovant l'existència de la cadena introduïda dins de les dades emmagatzemades als respectius camps a la base de dades. Aquests camps venen escrits per defecte amb les dades de l'empleat que ha iniciat sessió a l'aplicació. Però es poden editar per cercar els tràmits d'altres empleats de l'administració. Si els camps es deixen en blanc, no es tindran en compte a l'hora de fer el filtre a la base de dades.
- **Dates**: aquests camps fan referència a les dates d'alta, darrera modificació i tancament respectivament, dels diferents tràmits de la base de dades. La cerca retornarà els tràmits compresos entre les dates d'inici i fi que s'omplin al cercador. Si només s'omple la data

d'inici, es cercaran els tràmits amb data posterior a la data introduïda, i fins a l'actualitat. Si, en canvi, s'omple només la data de fi, es cercaran només aquells tràmits amb data anterior a la introduïda. Si els camps es deixen en blanc, no es tindran aquestes dates en compte a l'hora de realitzar la cerca. Per tant, no es filtraran els tràmits segons la seva antiguitat.

- **Estat**: aquest camp fa referència a l'estat del tràmit a la base de dades. Es tracta d'un desplegable que permetrà seleccionar si es volen mostrar els tràmits "Oberts", "En procés", "Tancats", "En Revisió", o "Anul·lats". Si es deixa el camp en blanc, no es tindrà en compte aquest criteri a l'hora de realitzar la cerca, per tant es mostraran els tràmits amb qualsevol estat que trobin a la base de dades.
- **Criteris d'ordenació. Ordenat per i De forma**: els criteris d'ordenació fan referència a la forma en que es vol que ens aparegui ordenada la llista de tràmits que ens retornarà la cerca a la base de dades. "Ordenat per" es refereix al camp pel qual volem ordenar. És a dir, si es tria el nom d'usuari, la taula de resultats ens apareixerà ordenada alfabèticament segons el nom d'usuari. Si es tria una data, estarà ordenada segons l'antiguitat d'aquella data. El criteri "De forma" fa referència al mètode d'ordenament. Si es tria ascendent, una cerca alfabètica serà mostrada des de la "A" fins a la "Z". Una cerca per data serà mostrada dels registres més antics al més nous. Si, en canvi, es marca l'opció descendent, l'ordenació alfabètica serà inversa, i la cerca per antiguitat anirà del tràmit més nou al més antic dels que formen part de la llista de tràmits cercats. Si es deixen en blancs aquests camps, la taula mostrarà el llistat de tràmits segons l'ordre en que han estat introduïts a la base de dades.

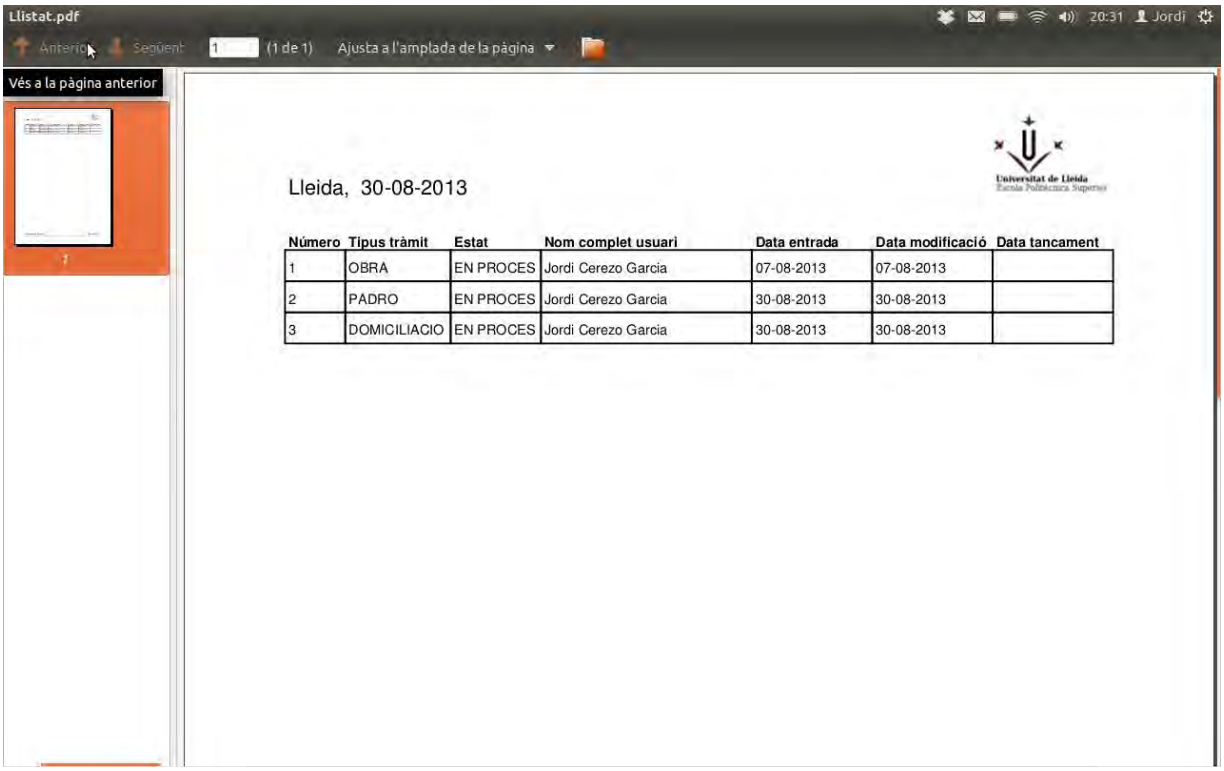
Per realitzar la cerca, s'ha de prémer el botó **"Cercar"**. El botó **"Reinicialitza"** restaura tots els camps del cercador al seu estat per defecte. El botó **"Sortir"** ens porta directament a la pantalla inicial de l'aplicació.

La llista de la part inferior de la pantalla contindrà, com s'ha esmentat anteriorment, els resultats de la la darrera cerca realitzada (Il·lustració 81).



Il·lustració 81: Cerca de tràmits amb llistat de resultats

La taula conté tots els resultats que s'adeqüen a la cerca realitzada. La darrera columna conté tres icones diferents a cada registre de la taula. La primera icona, amb una petita lupa, ens permet realitzar una consulta de les dades del tràmit. La segona icona, amb un petit llapis, ens permetrà realitzar una modificació de les dades del tràmit tractat. La darrera icona, amb una petita creu vermella, ens permetrà eliminar el registre corresponent, de tal manera que a la base de dades quedarà marcat com a desactivat. A la part inferior del llistat trobem dos botons. El botó **"Imprimir"** permetrà l'empleat crear un document de tipus pdf, amb el llistat de tràmits cercat (Il·lustració 82) i que podrà ser imprès en paper. El botó **"Sortir"** portarà l'empleat a la pàgina inicial de l'aplicació.



Número	Tipus tràmit	Estat	Nom complet usuari	Data entrada	Data modificació	Data tancament
1	OBRA	EN PROCES	Jordi Cerezo Garcia	07-08-2013	07-08-2013	
2	PADRO	EN PROCES	Jordi Cerezo Garcia	30-08-2013	30-08-2013	
3	DOMICILIACIO	EN PROCES	Jordi Cerezo Garcia	30-08-2013	30-08-2013	

Il·lustració 82: Document pdf amb impressió del llistat de tràmits

5.2.4.2 Gestió de tràmits

Després de la cerca, passarem a donar una explicació sobre la gestió dels diferents tipus de tràmits. Les diferents operacions que poden ser realitzades s'agruparan de forma independent al tipus de tràmit tractat, és a dir, una alta, una consulta, una modificació o una anul·lació d'un tràmit, seran iguals sense importar si parlem d'un permís d'obra o d'una llicència d'ús i ocupació. Existeixen petites diferències entre els diferents tipus de tràmits, així q primerament es farà una petita introducció als tràmits presents a l'aplicació.

El primer tipus de tràmit que veiem és el "**Padró d'habitants**". Amb aquest tipus de tràmit, una Administració pública pot emmagatzemar totes les dades referents als seus ciutadans, i realitzar un recompte en moments en que sigui necessari. S'ha de tenir en compte en el tràmit de tipus **"Padró"**, que, per a un ciutadà en particular, només pot existir un **"Padró" actiu**, i així quedarà reflectit a la base de dades. La resta de padrons inactius, es conservaran a la base de dades, a mode d'històric per als empleats de l'Administració Pública, per tal de saber les diferents residències per les que ha passat un ciutadà, però no seran accessibles per al propi ciutadà. Aquest, només tindrà accés al seu **"Padró" actiu**.

El segon tipus de tràmit que trobem a l'aplicació és el **"Permís d'obra"**. Aquest tràmit permet a un ciutadà sol·licitar a l'Administració el permís pertinent per dur a terme una obra en un immoble de la seva propietat. Quan disposi d'ell, podrà realitzar l'edificació, adequació o reforma de l'immoble. En aquest tràmit s'ha de remarcar l'existència de dues adreces diferents entre les dades que hi fan referència. El domicili del permís d'obra fa referència a l'adreça on està ubicat l'edifici on es realitzarà l'obra. El domicili de notificació fa referència a l'adreça on s'enviaran les notificacions referents al tràmit.

El tràmit **"Llicència d'Activitat"** permet a un ciutadà demanar a l'Administració una autorització per tal de realitzar activitats que poden suposar una incidència ambiental. Per tal de tenir un control sobre les possibles incidències que es puguin ocasionar al medi ambient, com ara la crema de rastrolls o el possible abocament de diverses substàncies a cursos de rius, l'Administració requereix a qualsevol ciutadà que fiqui en el seu coneixement aquestes activitats, per tal de poder realitzar les tasques de neteja o reparació en cas que es produeixi un abocament indegut o qualsevol altra incidència, i depurar responsabilitat davant greus atacs cap al medi ambient.

El tràmit **"Llicència d'Ús i Ocupació"** permet a un ciutadà la comunicació prèvia a l'Administració Pública de la primera utilització i ocupació d'edificis i construccions del nucli urbà. D'aquesta manera, l'Administració té un coneixement sobre quins dels edificis de la ciutat estan habitats i quins no, dada necessària per tal de gestionar els habitatges de la ciutat, i controlar la seva habitabilitat en benefici de la seguretat dels ciutadans.

El següent tràmit que pot ser gestionat a l'aplicació són les **"Sancions de la Guàrdia Urbana"**. Aquest tràmit, com el seu nom indica, permet a l'empleat la introducció i gestió de les sancions imposades per la Guàrdia Urbana de la ciutat. La sanció serà imposada pels agents , i els empleats de l'Administració introduiran la informació a la base de dades de l'aplicació. El ciutadà sancionat podrà introduir les seves dades bancàries per tal de poder realitzar el pagament de la sanció a través de domiciliació bancària.

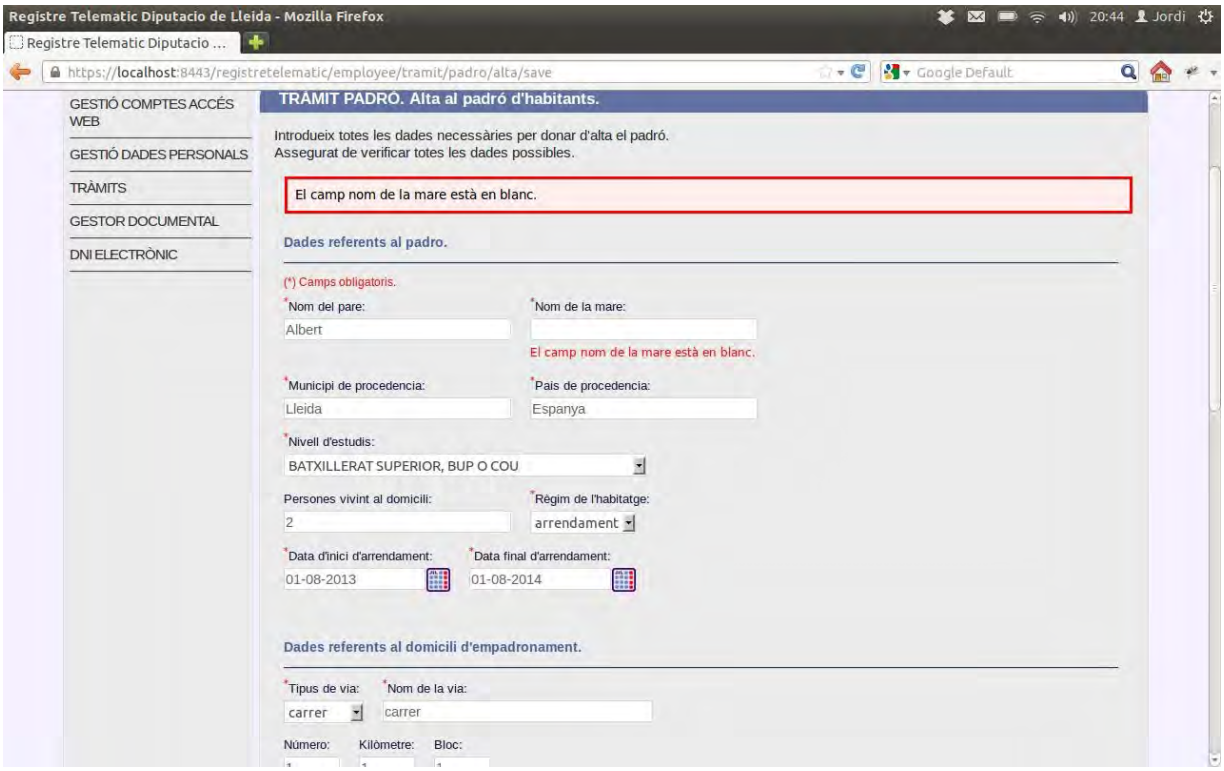
La **"Domiciliació de tributs"** és el següent tràmit que trobem a l'aplicació. En aquest cas, un ciutadà pot demanar a l'Administració que tots els pagaments de tributs, o bé algun d'ells de forma específica, pugui ser abonat a través de domiciliació bancària, aportant a l'Administració un número de compte bancari. Existeix la possibilitat de domiciliar els tribut en diversos comptes bancaris, creant diferents registres i marcant els tributs desitjats a cadascun d'ells per separat.

El darrer tràmit present a l'aplicació és l'**"Adreça Fiscal i/o de notificacions"**. L'Administració dona la possibilitat als ciutadans i empreses de la seva circumscripció d'aportar una adreça fiscal per tal de realitzar les tasques a nivell fiscal, o una adreça de notificacions per tal de mantenir informat al ciutadà de tot allò que li pot resultar necessari en quant a la seva activitat fiscal.

Passem seguidament a comentar cadascuna de les possibilitats en quant a la gestió dels tràmits de l'aplicació web. Les captures de pantalla correspondran a un únic tipus de tràmit, però aquestes imatges són extrapolables a qualsevol dels altres tipus.

5.2.4.2.1 Alta

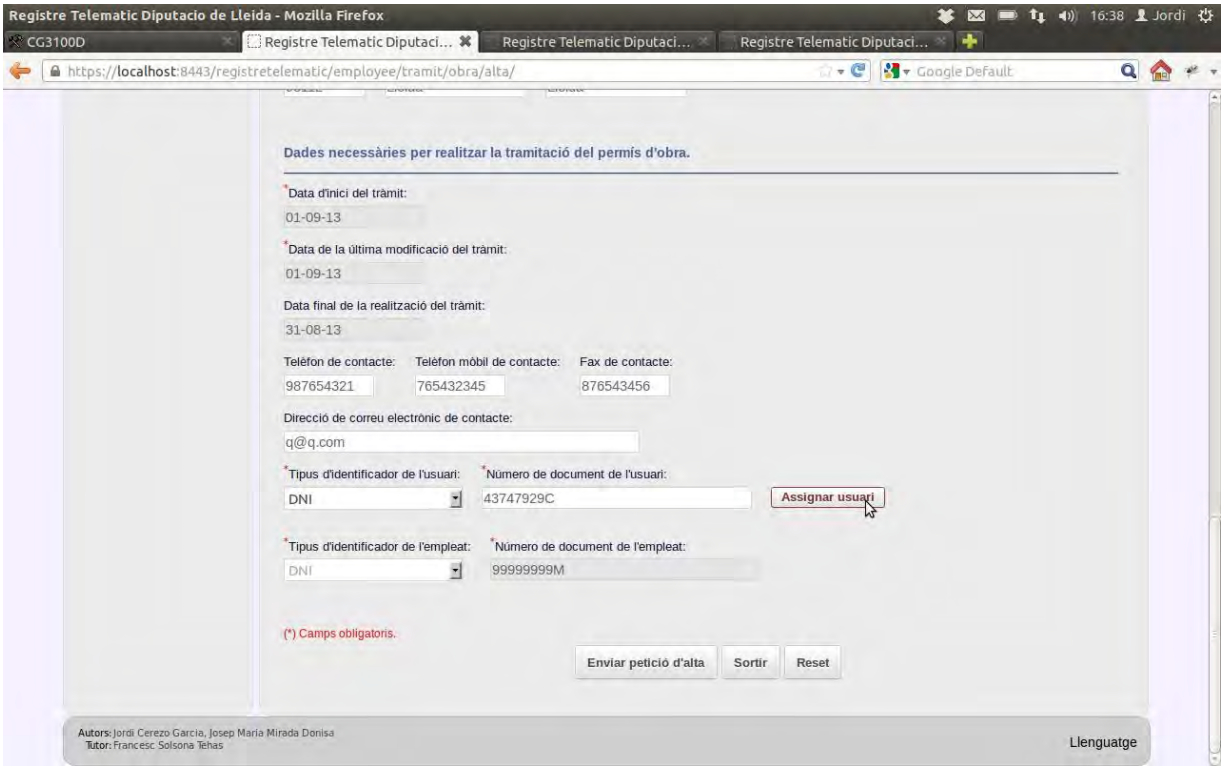
L'alta o creació d'un tràmit permet crear un nou registre del tipus de tràmit seleccionat a la base de dades introduint totes les dades necessàries, i que són sol·licitades als diferents formularis d'alta o creació. A la part inferior de la pantalla apareixen diversos botons. **"Sortir"** portarà l'empleat directament a la pantalla de benvinguda de l'aplicació. **"Reset"** reinicialitzarà les dades dels camps del formulari. En prémer el botó **"Enviar petició d'alta",** l'aplicació comprovarà la validesa de les dades introduïdes. En el cas que manqui alguna dada essencial (aquelles que estan marcades amb un asterisc vermell), o algun dels tipus de dades no sigui l'esperat, es marcarà amb missatges d'avís al propi formulari (Il·lustració 83). Quan totes les dades siguin vàlides, es durà a terme l'alta del tràmit a la base de dades.



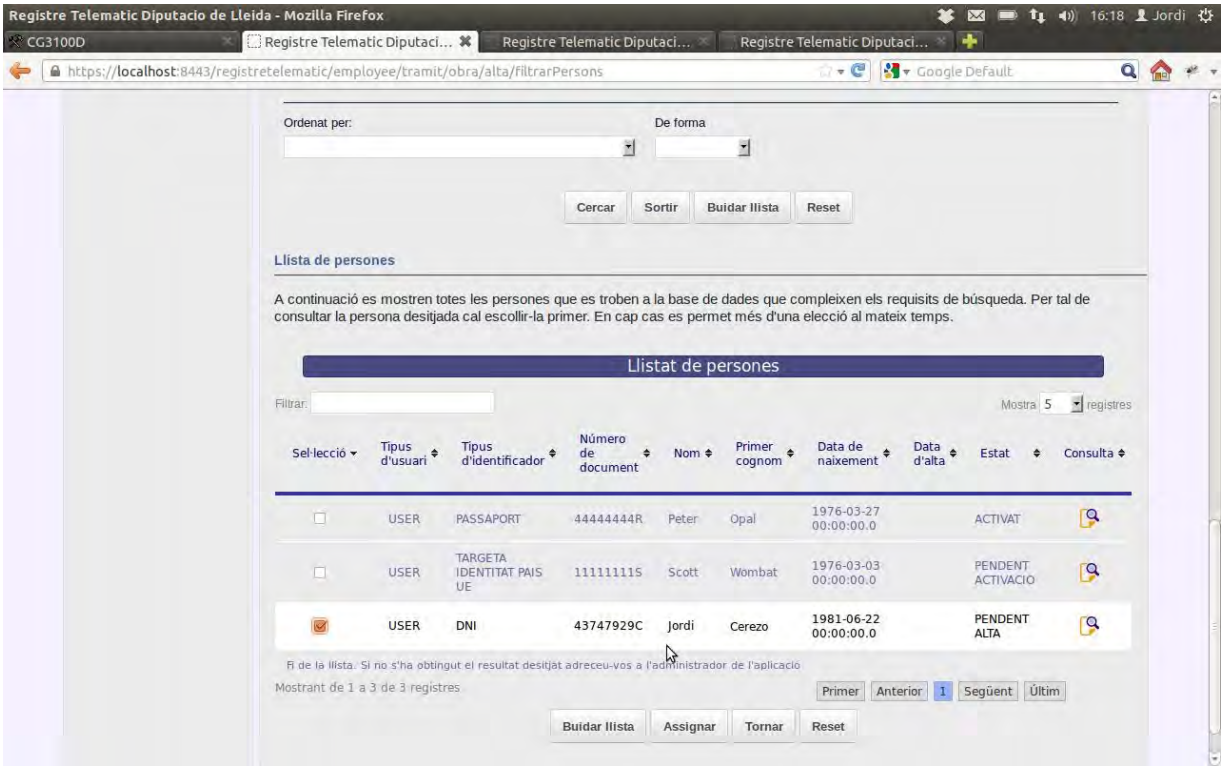
Il·lustració 83: Alta de tràmit (en aquest cas un padró) amb un error a la introducció de dades

A tots els tràmits se'ls hi ha d'associar un ciutadà, i a tal efecte hi ha dos camps al formulari, els quals recullen un tipus de document i un número de document, els quals acrediten a la base de dades la identitat del ciutadà. Per exemple, l'empleat podria seleccionar el tipus de document

"DNI", i escriure manualment el número de DNI del ciutadà al qual se li està creant el tràmit. Difícilment un empleat podrà recordar tots els números de documents dels ciutadans, i com existeix la possibilitat que el tràmit sigui creat sense la presència del ciutadà, s'ha donat la possibilitat d'assignar un ciutadà després de cerca-lo a la base de dades. L'empleat pot prémer el botó **"Assignar usuari"** (Il·lustració 84), i serà dirigit a una cerca de persones, de tipus "Usuari", que té el mateix funcionament que la resta de cerques de persones, i que ja han estat comentades en aquest manual(5.2.3.1 Cercador de persones). Després de prémer el botó **"Cercar"**, la taula inferior mostrarà els resultats obtinguts, i l'empleat podrà seleccionar un d'ells, marcant el checkbox de l'esquerra de la taula, i aquest ciutadà podrà ser assignat al tràmit que s'està creant prement el botó **"Assignar"** (Il·lustració 85). D'aquesta manera es retornarà cap a la pàgina de creació del tràmit, amb el tipus de document, i número de document, ja escrits als camps que designen l'usuari al qual pertanyerà el tràmit.

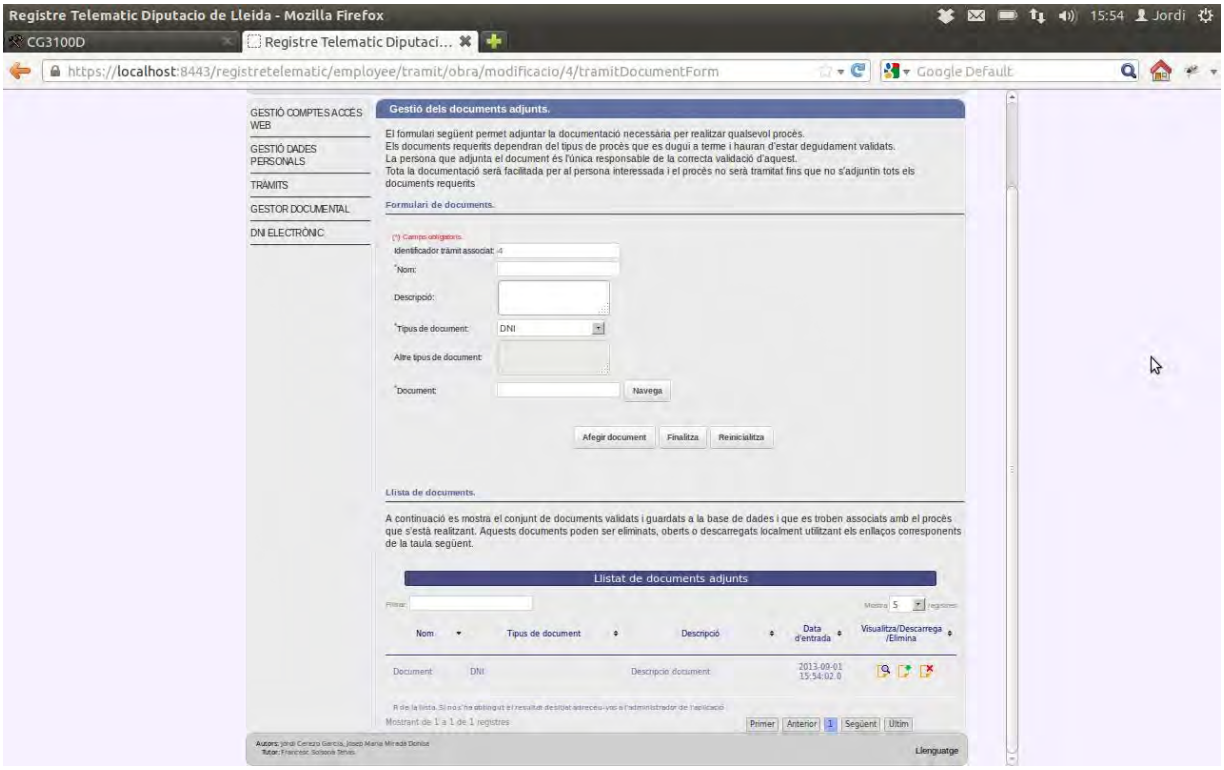


Il·lustració 84: Detall del botó d'assignació d'usuari al tràmit



Il·lustració 85: Assignació d'un ciutadà a un tràmit

Un cop donat d'alta el nou tràmit es mostrarà la finestra de **"Documentació"** (Il·lustració 86). Aquí es dona la oportunitat d'introduir documents referents al tràmit gestionat, en diferents formats per tal de tenir una còpia a la base de dades dels documents oficials que acrediten el tràmit creat, o al propi ciutadà depenent del cas. Els documents s'introdueixen posant el nom i descripció dels mateixos, i un diàleg de sistema operatiu per a cerca de documents a l'equip, permet pujar-lo a la base de dades de l'aplicació. Aquests quedaran reflectits a la taula inferior de la pantalla. Es farà un comentari en profunditat a l'apartat corresponent al gestor documental (5.2.5 Gestor documental).



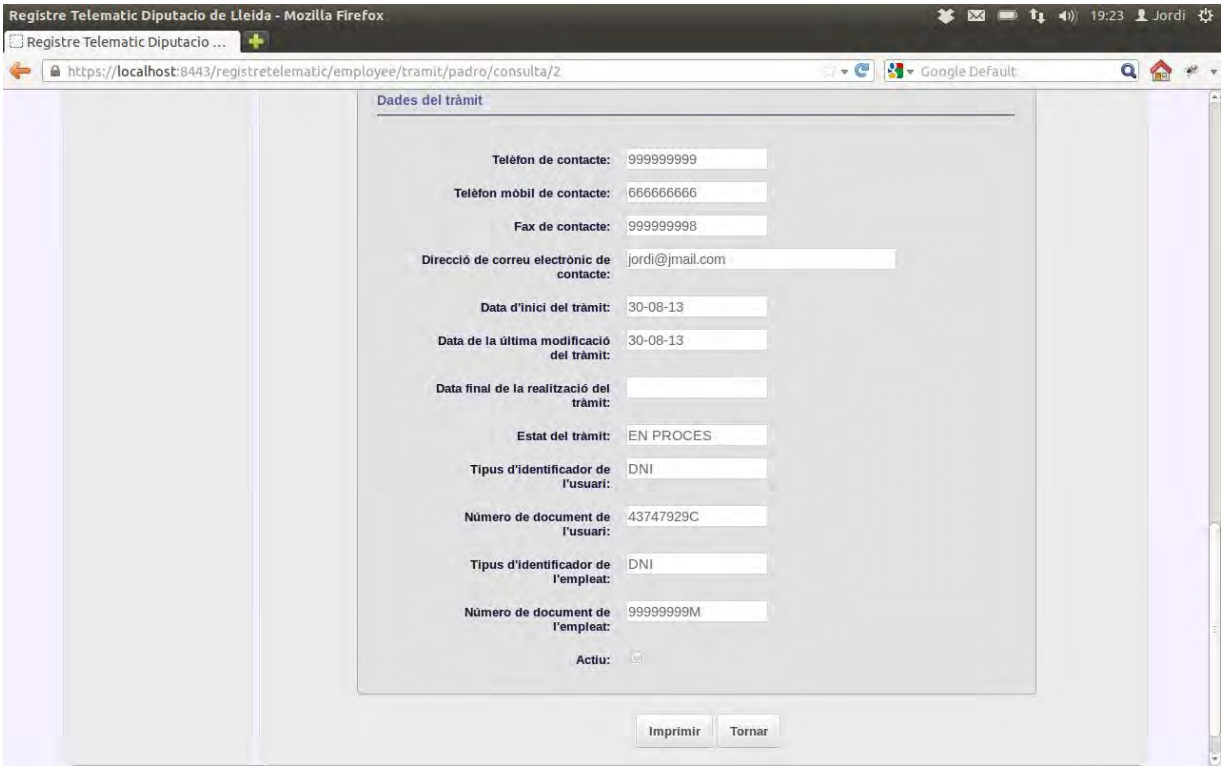
Il·lustració 86: Gestió de documents associats a un tràmit (en aquest cas un permís d'obra)

5.2.4.2.2 Consulta, modificació i anul·lació

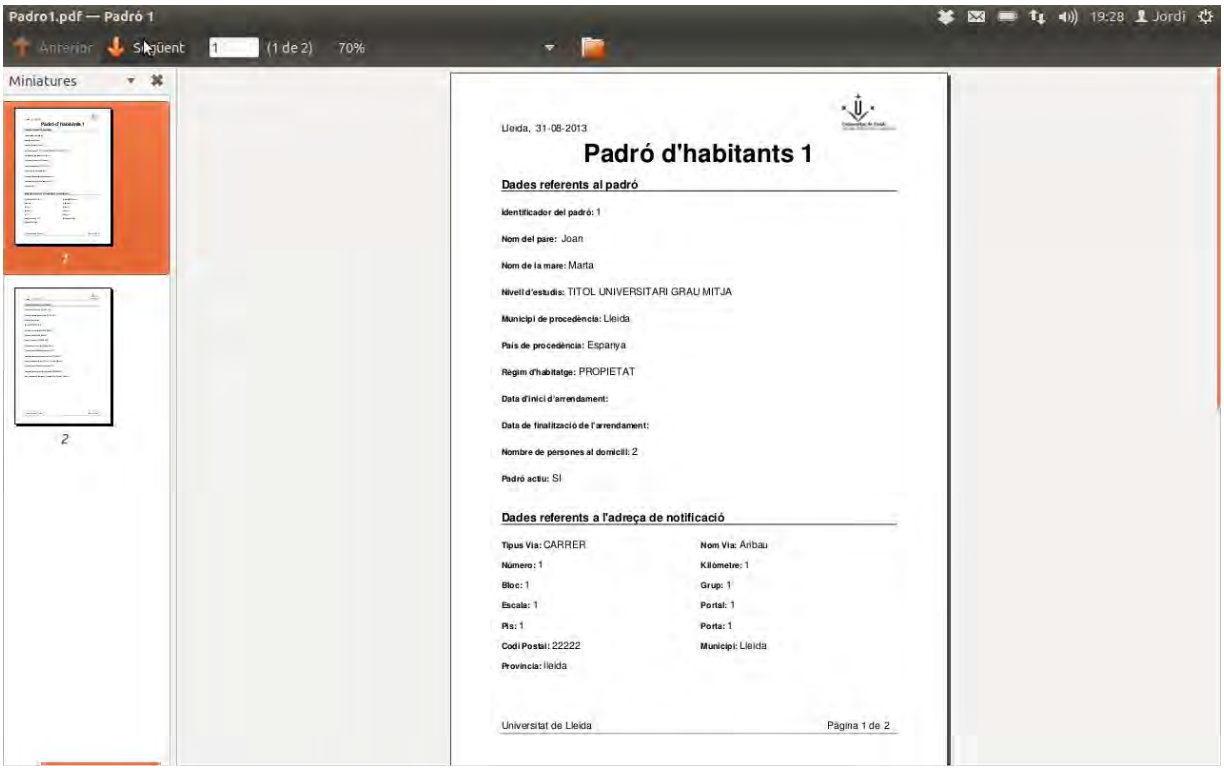
Els tres botons següents de les entrades de menú de cadascun dels tràmits portaran directament a una **cerca de tràmits** (5.2.4.1 Cercar qualsevol tràmit) amb la particularitat que el tipus de tràmit serà indefectiblement el que s'ha triat a l'entrada de menú. La cerca es realitzarà de la mateixa forma, i amb els mateixos criteris que una cerca global, però el camp **"Tipus Tràmit"** apareixerà en aquest cas deshabilitat, per tal d'assegurar que la cerca es realitza únicament sobre els tràmits del tipus seleccionat. A la part inferior, trobem el botó **"Reinicialitzar",** que tornarà a posar tots els camps del formulari al seu estat inicial i el botó **"Sortir"**, que ens portarà de nou a la pantalla de benvinguda de l'aplicació. Un cop escrits els criteris pels quals es vol realitzar la cerca a la base de dades, s'ha de prémer el botó **"Cercar"**. L'aplicació mostrarà a la taula de la part inferior del formulari, un llistat amb tots els tràmits del tipus seleccionat que compleixen els criteris prèviament seleccionats.

A la darrera de les columnes de la taula de resultats, marcada amb el títol **"Consulta/Modificació/Anul·lació"** apareixen tres icones, que permetran la consulta, modificació i anul·lació del tràmit seleccionat.

La icona de l'esquerra, marcada amb una petita lupa, porta a la pàgina de consulta del registre triat. En aquesta pantalla (Il·lustració 87) es poden consultar totes les dades referents al tràmit, sense possibilitat de modificar-lo. D'aquesta manera tenim la possibilitat de visualitzar les dades referents al tràmit sense el perill de modificar alguna dada de manera involuntària o accidental. Les dades mostrades en pantalla es poden imprimir en paper mitjançant el botó **"Imprimir"**, que generarà un document pdf que podrà ser obert amb qualsevol programa de visualització de pdf (Il·lustració 88). Un cop consultades les dades, es pot prémer el botó **"Tornar"**, i d'aquesta manera es tornarà al formulari de cerca amb totes les dades de la darrera cerca efectuades en pantalla.

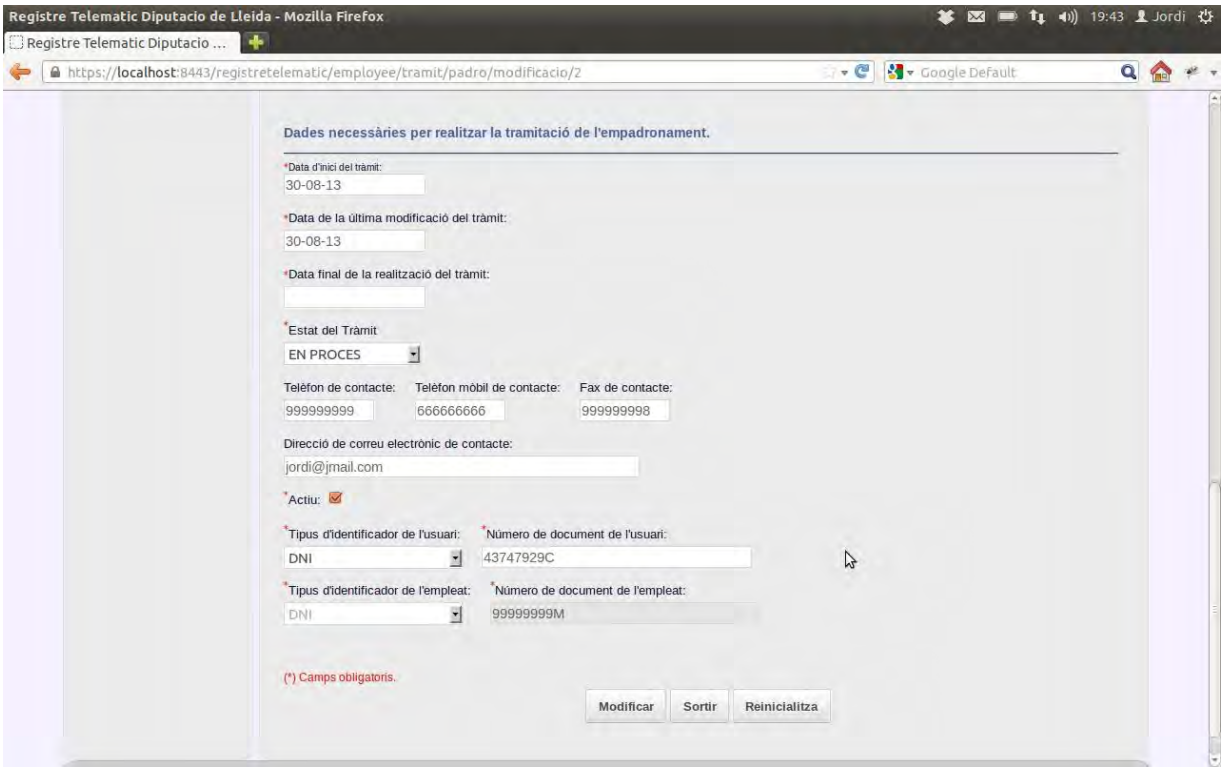


Il·lustració 87: Consulta de tràmit (en aquest cas un padró d'habitants), detall de botons inferiors



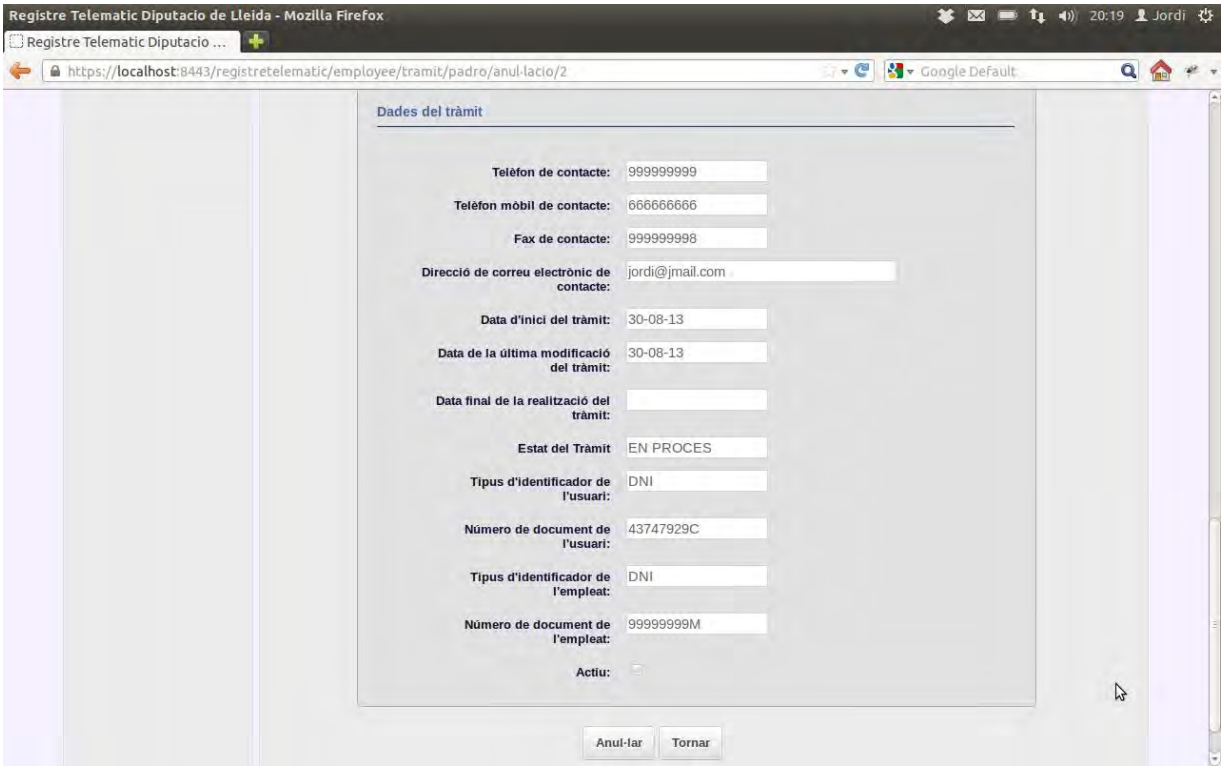
Il·lustració 88: Pdf consulta de tràmit (en aquest cas un padró d'habitants)

La icona central de la taula de resultats, la que conté un petit llapis, portarà directament a la pàgina de **modificació del tràmit** escollit. Aquesta pantalla (Il·lustració 89) mostra totes les dades referents al tràmit seleccionat, però en aquest cas les dades sí que es poden modificar. El botó **"Sortir"** portarà directament a la pantalla de benvinguda. El botó **"Reinicialitzar"** buidarà tots els camps del formulari, per tal de tornar a introduir tota la informació de nou. Un cop realitzats els canvis desitjats, s'ha de prémer el botó **"Modificar"**. Les dades seran validades. En el cas que alguna dada essencial, les que estan marcades amb un asterisc vermell, no sigui introduïda, o bé el tipus de dada sigui incorrecte, es mostraran els missatges d'error al propi formulari. Un cop les dades siguin vàlides, el tràmit serà introduït a la base de dades, i es passarà a la pantalla d'introducció de documents referents al mateix (Il·lustració 86). Es parlarà en profunditat del gestor documental més endavant en aquest manual (5.2.5 Gestor documental).



Il·lustració 89: Modificació de tràmit (en aquest cas un padró d'habitants), detall dels botons

La icona de l'esquerra de la taula de resultats, la que conté una petita creu vermella, portarà directament a la pàgina d'**anul·lació del tràmit** escollit. Aquesta pantalla (Il·lustració 90) mostra totes les dades referents al tràmit seleccionat. En aquest cas les dades no es poden modificar. El botó **"Tornar"** retornarà l'empleat a la pantalla anterior, amb les dades de la darrera cerca que s'ha realitzat. El botó **"Anul·lar"** marcarà aquest tràmit com a anul·lat, i no serà vàlid a l'aplicació. Cal remarcar que el tràmit no serà eliminat de la base de dades, per evitar pèrdues involuntàries d'informació, si no que únicament quedarà marcat amb estat **"ANUL·LAT"**. En anul·lar un tràmit, es mostrarà una pantalla informant que la operació ha estat correcta.

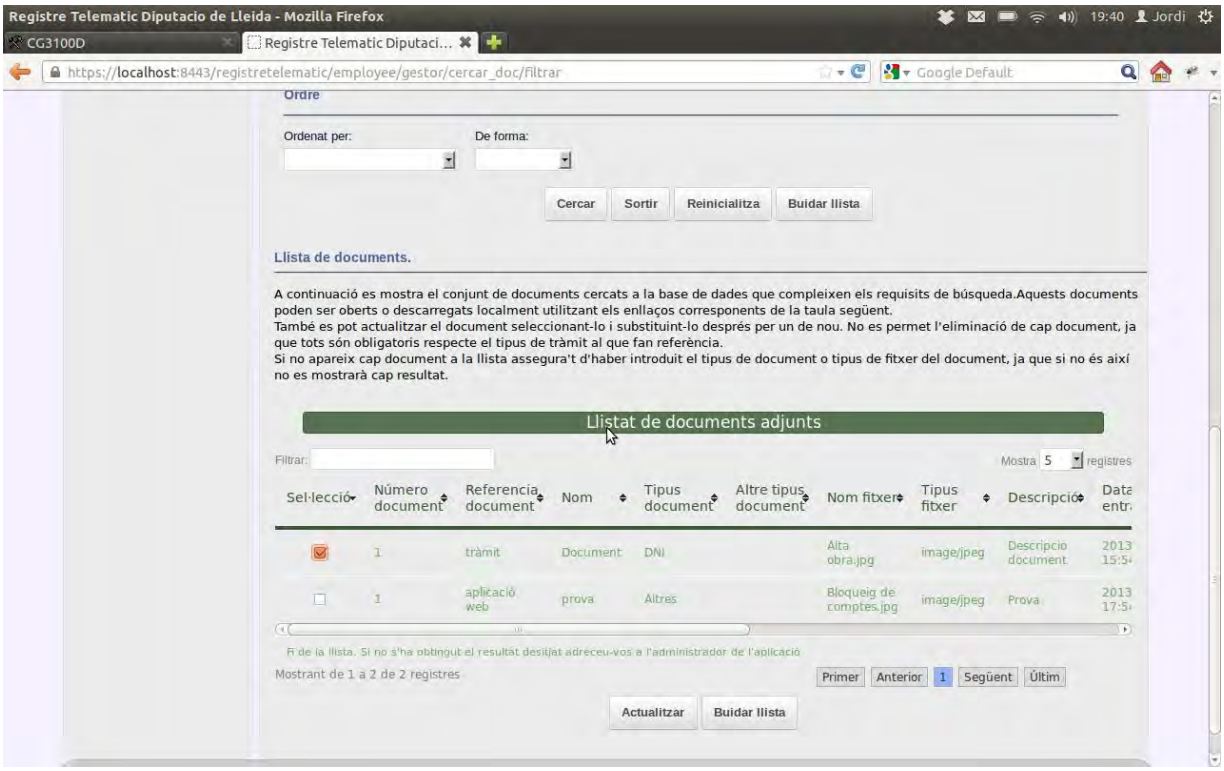


Il·lustració 90: Anul·lació de tràmit (en aquest cas un padró d'habitants), detall dels botons

5.2.5 Gestor documental

El **gestor documental** (Il·lustració 91) és la part de l'aplicació encarregada de la gestió de documents acreditatius de la identitat dels ciutadans i empleats de la base de dades, així com de qualsevol document que faci referència a algun dels tràmits que gestiona l'aplicació web. Els documents no són necessaris en cap cas per a la creació o gestió dels tràmits o persones, però moltes vegades és important tenir documents que serveixin per contrastar determinades dades. Per exemple, en el cas d'introduir a l'aplicació un perfil d'una persona, o un tràmit de tipus padró, pot ser interessant emmagatzemar una copia del DNI. En el cas de demanar un permís d'obra, pot ser convenient emmagatzemar una còpia de l'expedient d'obra, i en el d'una sanció de la guàrdia urbana, podria ser convenient guardar la imatge escanejada de la còpia de l'agent.

Aquest gestor documental té la capacitat d'emmagatzemar documents de tota mena. La base de dades es limitarà a guardar-los, donant la possibilitat de la seva posterior visualització o descàrrega. Per poder obrir el document cal disposar a l'ordinador d'un programa amb la capacitat per obrir el document seleccionat. Per exemple, si el document és de tipus JPG, serà necessari disposar d'un visualitzador d'imatges capaç d'obrir documents d'aquest tipus. Si el document és un text en format ODT, serà necessari disposar d'una aplicació amb capacitat d'obrir documents de text d'aquest format.



Il·lustració 91: Exemple del resultats d'una cerca global del gestor documental

Cal remarcar que, aquest gestor documental té la capacitat d'emmagatzemar documents **relacionats amb les persones,** o bé documents **relacionats amb els tràmits**. Els dos tipus seran accessibles des de l'entrada de menú etiquetada com a **"Gestor Documental"**, i podran ser cercats conjuntament, o bé delimitant-los segons el tipus de registre amb el que tenen relació, això és, persones o tràmits.

Segons l'entrada de menú que seleccioni l'empleat, el formulari de cerca variarà els camps que

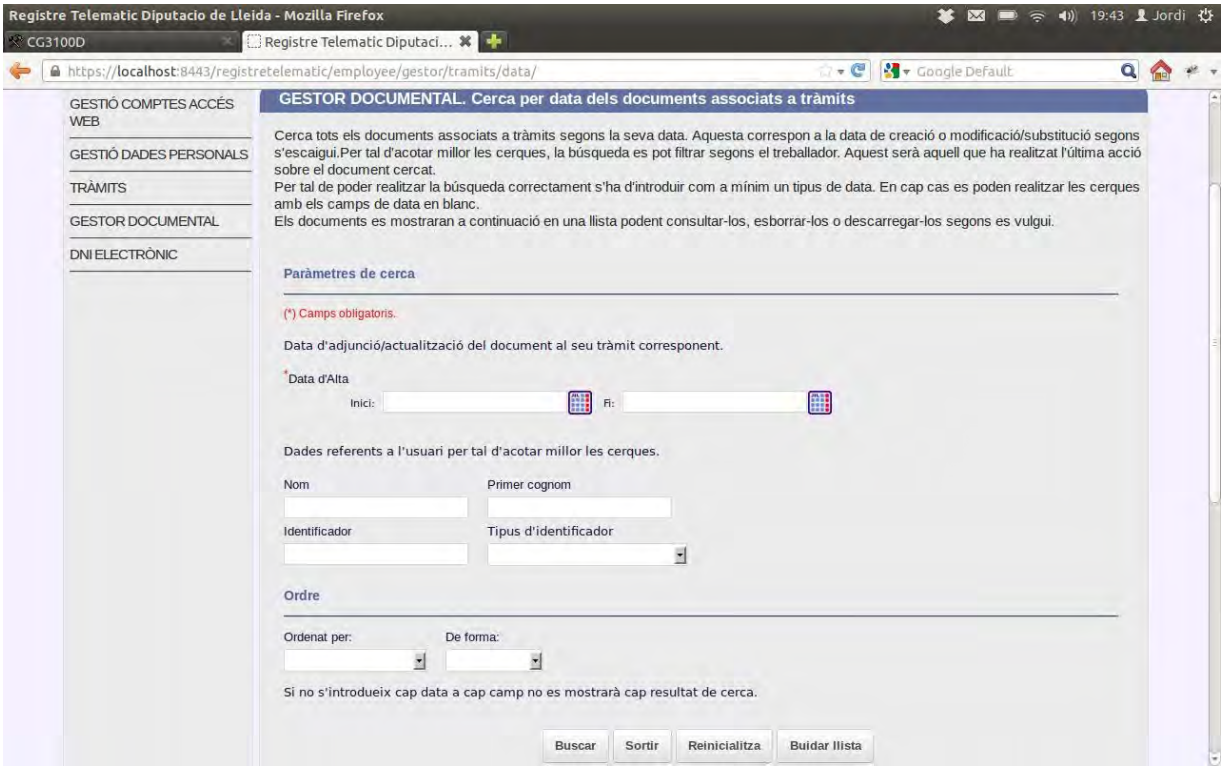
acoten els resultats, des de una cerca per dates, a una cerca per usuari o empleat. El funcionament del gestor documental serà en tots els casos el mateix. L'empleat podrà escriure els valors als camps del formulari de cerca pels quals vol acotar el filtratge. Existeixen diversos botons a la part inferior. El botó **“Sortir”** portarà l'empleat a la pantalla de benvinguda. El botó “**Reinicialitzar”** retornarà tots els camps del formulari al seu estat inicial. El botó **“Buida llista”** eliminarà tots els registres de la taula de resultats inferior. Mitjançant el botó **“Cercar”,** la taula de la part inferior serà carregada amb els resultats que compleixen les restriccions. La funcionalitat més important d'aquesta taula de resultats la trobem a la darrera columna dels registres mostrats. Aquí trobem tres icones, les quals permetran a l'empleat realitzar la gestió dels documents. La icona de l'esquerra, amb una petita lupa, permetrà visualitzar el document seleccionat utilitzant el programa amb capacitat per la lectura del format de document triat. La icona central, marcada amb una petita fletxa verda apuntant cap a baix, permetrà l'empleat descarregar una còpia del fitxer seleccionat, i guardar-lo a la carpeta de l'ordinador que trii. Finalment, la icona de la dreta, marcada amb una petita creu vermella, permetrà l'eliminació del document seleccionat de la base de dades.

Aquesta explicació de la funcionalitat dels cercadors de documents serà vàlida per a tots els casos que passem a comentar amb més profunditat seguidament.

5.2.5.1 Documents referents a tràmits

La primera entrada del menú fa referència a documents relacionats a tràmits. Per tant, ens referim a documents que s'han introduït acreditant dades d'un tràmit, i no d'una persona. Podem realitzar la cerca mitjançant diferents paràmetres, depenent de la entrada de menú escollida:

- **Cerca per data** (Il·lustració 92)**:** permetrà a l'empleat realitzar una cerca dels documents associats a tràmits, acotant els resultats mitjançant la **data d'introducció** a l'aplicació. La data inicial fa referència a documents que hagin estat introduïts amb posterioritat a la data seleccionada. La data final es refereix a documents que hagin estat introduïts amb anterioritat a la data seleccionada. En aquest cas, el valor de la data d'alta inicial ha de contenir un valor, o l'aplicació ens mostrarà un error en prémer el botó “Cercar”, informant al propi formulari dels errors.
- **Cerca per empleat**: permetrà realitzar una cerca marcant el nom i cognoms d'un empleat determinat, o be el tipus de document i número que l'acrediten a la base de dades, per exemple, el seu DNI. En aquest cas, si el nom de l'empleat no s'introdueix, l'aplicació mostrarà un error al propi formulari.
- **Cerca per usuari**: permetrà realitzar una cerca marcant el nom i cognoms d'un ciutadà determinat, o be el tipus de document i número que l'acrediten a la base de dades, per exemple, el seu DNI. En aquest cas, si el nom de l'usuari no s'introdueix, l'aplicació mostrarà un error al propi formulari.
- **Cerca per tipus de tràmit i estat**: permetrà realitzar una cerca de documents segons el tipus de tràmit al que estan associats, així com el seu estat a la base de dades. En aquest cas, si el tipus de tràmit o l'estat del mateix no s'introdueixen, l'aplicació mostrarà un error al propi formulari.

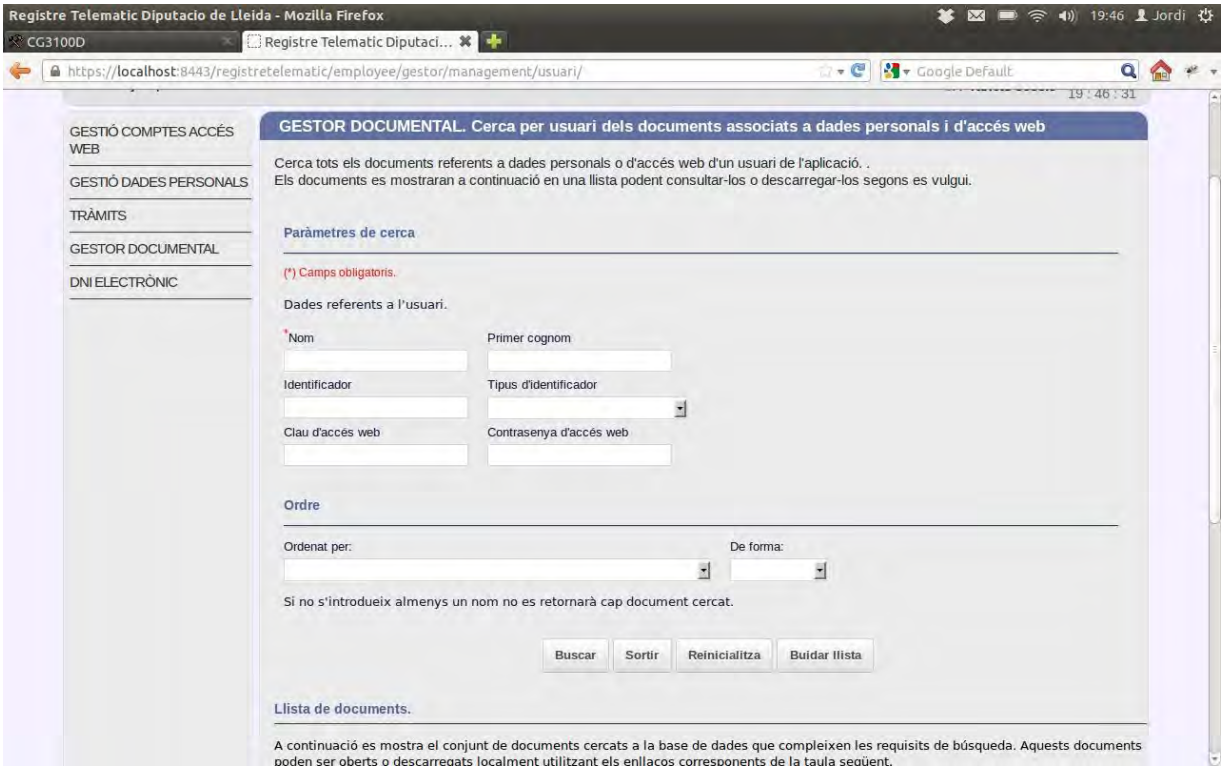


Il·lustració 92: Gestor documental. Cerca per data de documents associats a un tràmit

5.2.5.2 Documents referents a dades personals o dades d'accés a la web

Aquesta entrada del menú fa referència a tràmits associats a persones, usuaris de la pàgina web. Per tant, ens referim a documents acreditatius de la identitat personal dels usuaris. Depenent de la entrada de menú escollida podem realitzar la cerca per diversos paràmetres:

- **Cerca per data**: permetrà a l'empleat realitzar una cerca dels documents associats a persones, acotant els resultats mitjançant la **data d'introducció** a l'aplicació. La data inicial fa referència a documents que hagin estat introduïts amb posterioritat a la data seleccionada. La data final es refereix a documents que hagin estat introduïts amb anterioritat a la data seleccionada. En aquest cas, el valor de la data d'alta inicial ha de contenir un valor, o l'aplicació ens mostrarà un error en prémer el botó **"Cercar"**, informant al propi formulari dels errors.
- **Cerca per usuari**: (Il·lustració 93) permetrà realitzar una cerca de documents associats a persones, marcant el nom i cognoms d'un ciutadà determinat, o el tipus de document i número que l'acrediten a la base de dades, per exemple, el seu DNI, o bé per les seves dades d'accés a la web, es a dir , el seu nom d'usuari i contrasenya. En aquest cas, si el nom de l'usuari no s'introdueix, l'aplicació mostrarà un error al propi formulari.
- **Cerca per tipus de document**: permetrà realitzar una cerca de documents associats a persones, acotant els resultats segons el tipus de document que acredita al ciutadà. Per exemple, pot cercar només DNI's, o bé només passaports. Si el tipus de document no s'introdueix, l'aplicació mostrarà un error al propi formulari.



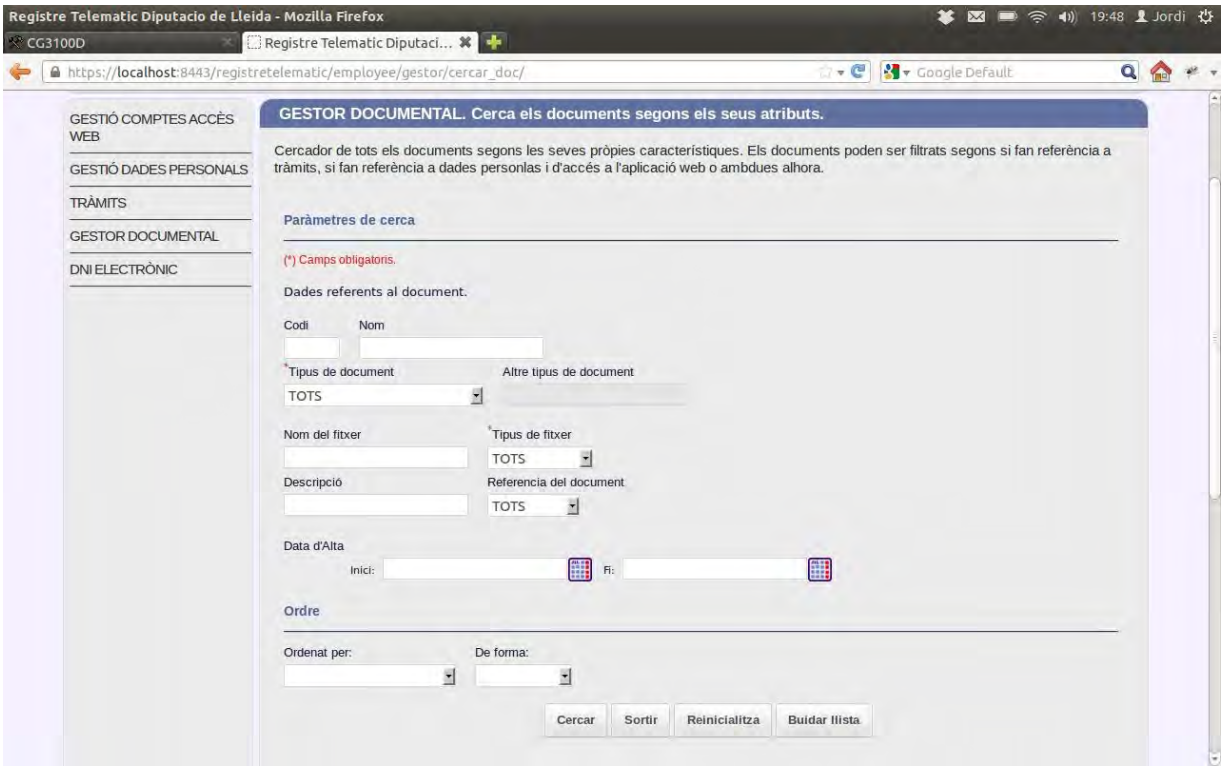
Il·lustració 93: Gestor documental. Cerca per usuari de documents acreditatius d'identitat

5.2.5.3 Cercar documents

Aquesta entrada de menú permet realitzar la cerca de documents més global de l'aplicació. Portarà a l'empleat a un formulari de cerca, que podrà emplenar per tal d'acotar els resultats de la cerca (Il·lustració 94). Els valors que pot seleccionar són:

- **Codi**: fa referència al codi associat al document a la base de dades. Si l'empleat coneix el codi del document, generat de manera automàtica durant la seva inserció a la base de dades i mostrat al formulari d'inserir documents adjunts, aquesta és la forma més ràpida de cercar-lo.
- **Nom**: fa referència al nom del document que se li va assignar al introduir-lo a la base de dades.
- **Tipus de document**: fa referència al tipus de document acreditatiu de la identitat dels usuaris a la base de dades de l'aplicació. L'empleat pot cercar, per exemple, només documents de tipus DNI, passaport o llibre de família entre altres. Si al desplegable se selecciona l'entrada "ALTRES", s'habilitarà el camp **"Altre tipus de document"**, per tal d'introduir manualment el tipus de document desitjat.
- **Nom del fitxer**: fa referència al nom real del fitxer, el que tenia al sistema de fitxers del sistema operatiu en el moment de guardar-lo al gestor documental. S'ha de diferenciar del "nom", que es refereix al nom que l'empleat va introduir a la base de dades per tal d'emmagatzemar-lo.
- **Tipus del fitxer**: fa referència al tipus de fitxer que s'està cercant, per exemple, imatges o documents pdf entre altres.

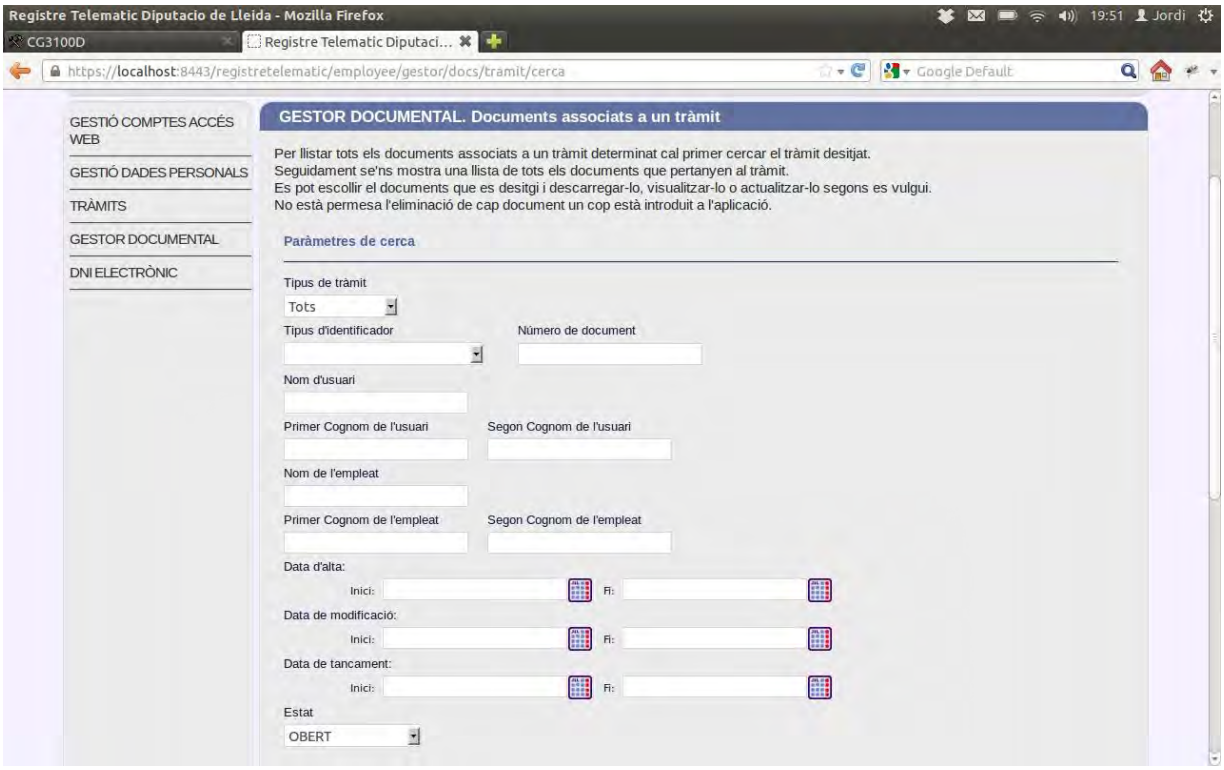
- **Descripció**: fa referència a la descripció que l'empleat va introduir al guardar el document a la base de dades.
- **Referència del document**: aquest camp permet diferència entre els documents que estan associats a un usuari de l'aplicació, o bé a un tràmit.
- **Criteris d'ordenació. Ordenat per i De forma**: els criteris d'ordenació fan referència a la forma en que es vol que ens aparegui ordenada la llista de tràmits que ens retornarà la cerca a la base de dades. “Ordenat per” es refereix al camp pel qual volem ordenar. És a dir, si es tria el nom d'usuari, la taula de resultats ens apareixerà ordenada alfabèticament segons el nom d'usuari. Si es tria una data, estarà ordenada segons l'antiguitat d'aquella data. El criteri “De forma” fa referència al mètode d'ordenament. Si es tria ascendent, una cerca alfabètica serà mostrada des de la “A” fins a la “Z”. Una cerca per data serà mostrada dels registres més antics al més nous. Si, en canvi, es marca l'opció descendent, l'ordenació alfabètica serà inversa, i la cerca per antiguitat anirà del tràmit més nou al més antic dels que formen part de la llista de tràmits cercats. Si es deixen en blancs aquests camps, la taula mostrarà el llistat de tràmits segons l'ordre en que han estat introduïts a la base de dades.



Il·lustració 94: Gestor documental. Cercador de tots els tipus de document

5.2.5.4 Documents associats a un tràmit

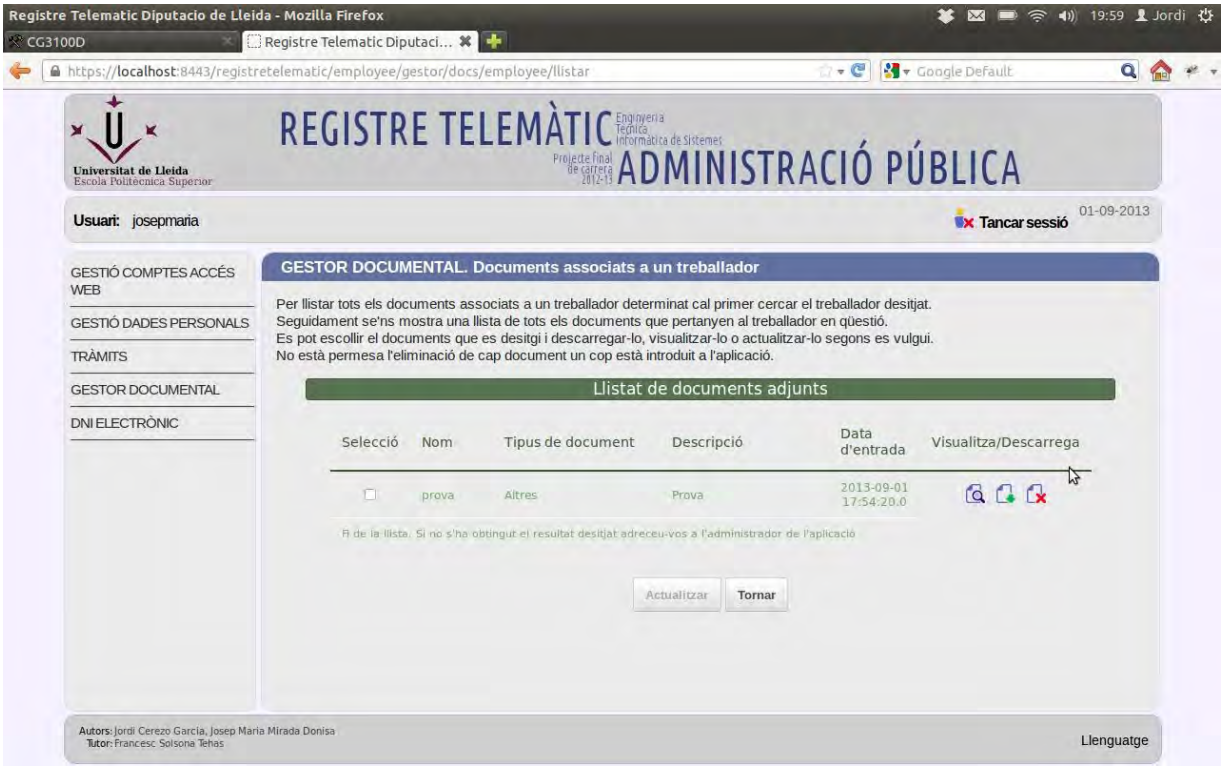
Aquesta entrada de menú permetrà cercar documents associats a un determinat tràmit emmagatzemat a la base de dades. Per fer-ho, en primer lloc l'empleat serà adreçat a una cerca de tràmits. Després de completar els camps pels quals vol filtrar, haurà de seleccionar un tràmit a la taula de resultats. Finalment, prement el botó inferior **"Llistar documents adjunts"** l'aplicació mostrarà en pantalla una finestra amb un una taula llistant tots els documents referents al tràmit seleccionat (Il·lustració 95). Si no hi ha cap document associat, aquesta taula simplement apareixerà buida.



Il·lustració 95: Gestor documental. Documents associats a un tràmit

5.2.5.5 Documents associats a un usuari, empleat o administrador

Les darreres tres entrades del menú del gestor documental permeten realitzar la cerca de documents associats a un usuari de la base de dades. Depenent de si es tria documents associat a un usuari, a un empleat o a un administrador, l'aplicació portarà a un formulari en el qual podem escriure les dades d'un usuari determinat. Els resultats seran mostrats en la taula inferior. Un cop se seleccioni un d'ells, es podrà prémer el botó inferior **"Llistar documents adjunts"**, que mostrarà una pantalla amb els documents associats a l'usuari escollit (Il·lustració 96). Si aquest usuari no té cap document acreditatiu introduït a la base de dades, la taula de resultats apareixerà buida.



Il·lustració 96: Gestor documental. Documents associat a un usuari (en aquest cas un empleat)

5.2.6 DNI Electrònic

Aquesta darrera entrada de menú permetrà la comprovació dels certificats d'autenticació i de signatura del DNI-electrònic. D'aquesta manera, en cas que no es pugui dur a terme alguna de les tasques associades al DNI-e, podrem determinar si existeix alguna mena d'error en els certificats emmagatzemats al xip del DNI. Tant per al certificat d'autenticació com per al de signatura, l'empleat podrà realitzar tres accions diferents:

- **Visualitzar les dades**: mostrarà les dades contingudes al certificat.
- **Comprovar l'estat**: mostrarà l'estat del certificat, de tal manera que l'empleat podrà conèixer si ha estat revocat, o si és vigent en el moment en que es realitza la comprovació.
- **Comprovar la data d'expiració**: mostrarà la data en que el certificat deixarà de ser vàlid. D'aquesta manera, l'empleat podrà advertir al ciutadà del moment en que expirarà, i aquest podrà renovar-lo abans que la revocació sigui executada.

Per evitar la duplicitat en l'explicació sobre el funcionament dels botons de comprovació dels certificats, adrecem a l'empleat a l'apartat "5.3.6 DNI Electrònic" del manual d'instruccions dels "Usuaris".

5.3 Usuari

5.3.1 Pantalla inicial

En la pantalla inicial (Il·lustració 97) de l'aplicació per a l'usuari, trobem un menú a la part esquerra, que serà el mètode d'accés a totes les possibilitats que ens proporciona el programa de registre telemàtic. Navegant per aquest menú podrem realitzar totes aquelles tasques necessàries per a la creació, emmagatzemament, consulta i modificació de les dades necessàries per al bon funcionament de l'aplicació. Entre les més importants trobem la gestió de les dades personals de l'usuari, i la gestió dels tràmits creats pel ciutadà i posats a disposició de l'usuari per l'Administració Pública corresponent, i de la documentació associada a aquests tràmits, i que també poden ser desats a la base de dades de l'aplicació.

En aquesta pantalla inicial es mostra una taula que conté un llistat de tots aquells tràmits de l'usuari que ha iniciat sessió, que requereixen ser signats per diversos motius. El més habitual serà una modificació de les dades contingudes al tràmit, i dutes a terme per un empleat de l'Administració. La signatura continguda al registre va ser creada amb les dades originals, però davant un canvi d'aquestes dades, la signatura passarà a ser obsoleta, i caldrà que el ciutadà signi les dades de nou. La taula que conté aquestes dades té diverses funcionalitats pròpies. A la part superior esquerra hi ha una caixa de text mitjançant la qual es poden filtrar els resultats de la taula, amb a finalitat d'afinar encara més la cerca. A la part superior dreta es pot introduir el número de registres que es volen mostrar a cada pàgina de la taula. A la part inferior dreta hi ha una sèrie de botons que permeten la navegació a través dels registres de la taula, portant a l'usuari de forma directa a la primera pàgina, la pàgina anterior, la pàgina següent, la pàgina final, i qualsevol d'elles de manera directa, mitjançant el seu número. Totes les taules de resultats de l'aplicació són similars i tindran les mateixes funcionalitats per a recórrer els resultats.

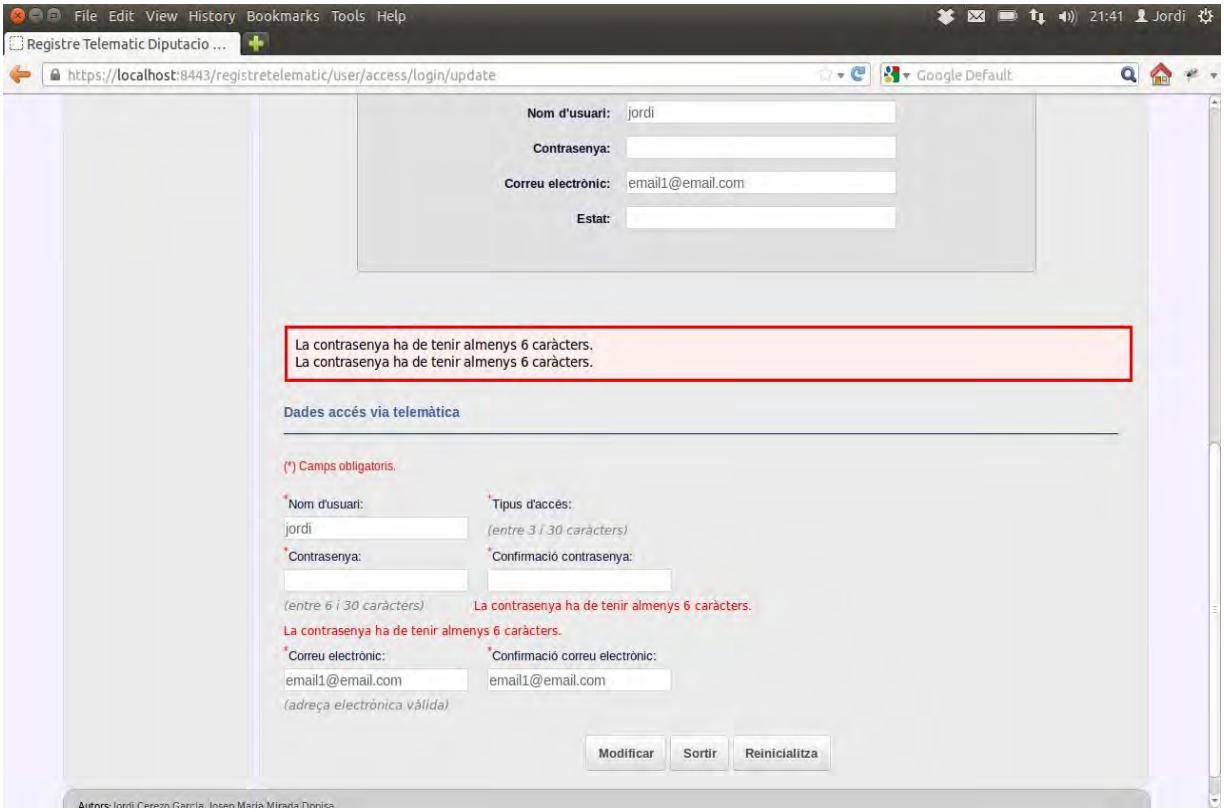
Il·lustració 97: Pantalla inicial de l'usuari

També podem observar en aquesta pantalla inicial de l'aplicació web, el botó anomenat “Tancar Sessió”. Com indica la seva etiqueta, aquest botó serveix per tancar la nostra sessió a l'aplicació, i retornar-nos a la pantalla d'accés al programa, on es pot introduir el nom d'usuari i contrasenya, o bé el DNI-e, i el seu PIN. Passem seguidament a comentar les entrades del menú contextual de l'esquerra de la pantalla, i que ens permetran fer ús de l'aplicació.

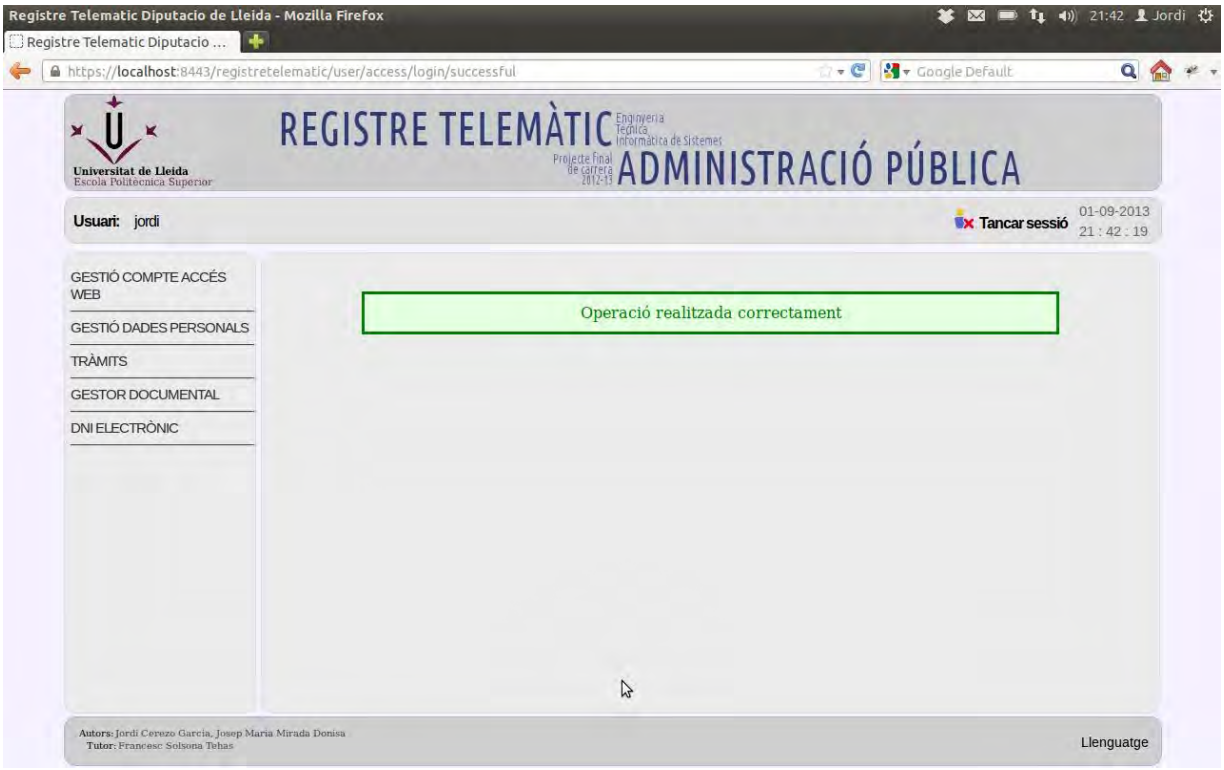
5.3.2 Gestió de compte d'accés web

La primera entrada del menú lateral, permetrà al ciutadà **“Gestió de compte d'accés a la web”**, és a dir, la gestió del seu compte d'usuari, i que li permet l'accés a l'aplicació. En prémer aquest botó, es desplegarà el menú associat amb una sèrie d'entrades que ens faciliten l'esmentada gestió.

La primera, etiquetada com **“Consultar i modificar el meu nom d'usuari i contrasenya”**, ens permetrà al ciutadà la consulta i modificació de les dades del compte d'accés a la pàgina web. A la part superior es mostren les dades de la persona associada al compte web, i a la part inferior, les dades del compte d'accés. Aquestes són les dades que poden ser alterades. Per tal de fer-ho, s'han de escriure les noves dades a les caixes de text, i prémer el botó “Modificar”. Si les dades són incorrectes, es mostrarà un missatge d'error a la vora de les caixes de text on s'ha detectat l'error informant a l'usuari del problema (Il·lustració 98). Si les dades no presenten cap error, es mostrarà un missatge informant de la correcta modificació (Il·lustració 99).

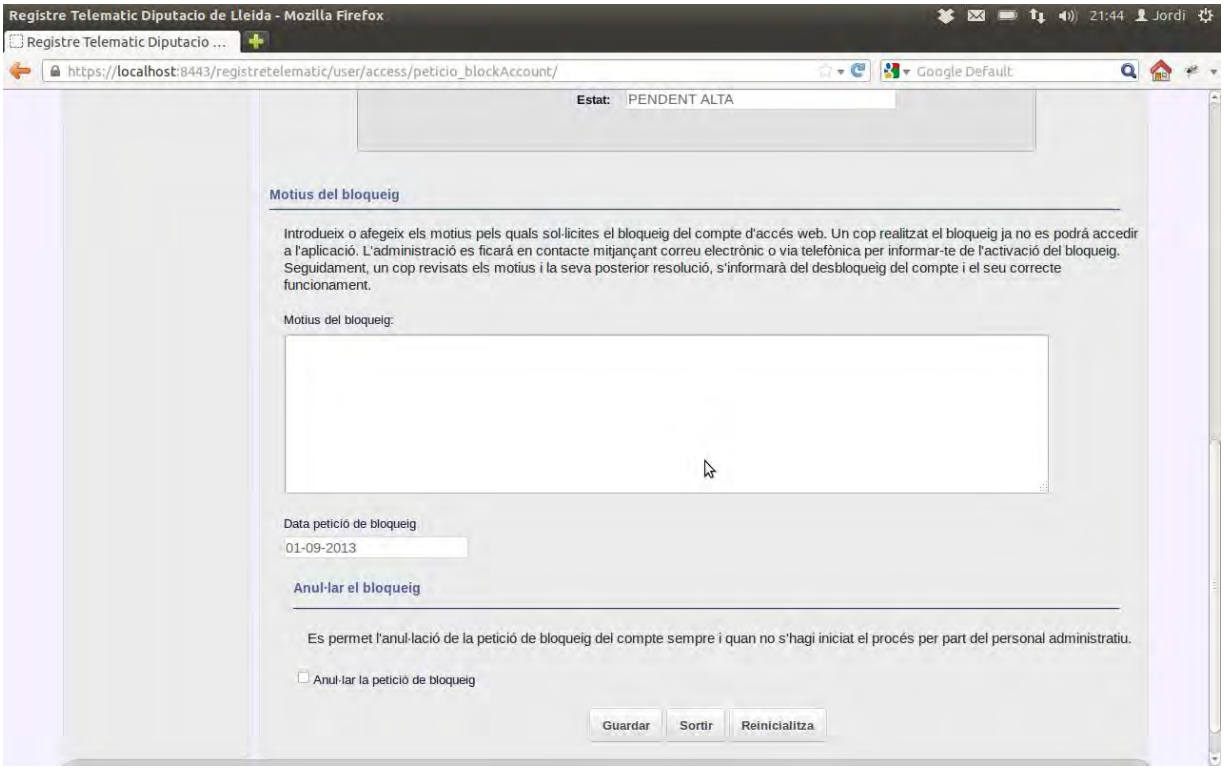


Il·lustració 98: Gestió del compte d'accés web mostrant un error a les dades introduïdes



Il·lustració 99: Modificacióó del compte web del ciutadà mostrant l'èxit en la operació de modificació

El segon botó etiquetat com a **“Bloquejar el meu compte”** permet al ciutadà demanar el bloqueig del seu propi compte(Il·lustració 100) per veure la seguretat compromesa davant d'una subtracció de les dades d'accés. A la part inferior de la pantalla es demanen els motius pels quals es vol donar de baixa el compte, cosa q es realitza prement el botó **“Guardar”**. També és visible un checkbox que permet, activant-lo, anul·lar una petició de bloqueig, sempre que el procés no hagi estat iniciat pel personal administratiu de l'Administració.



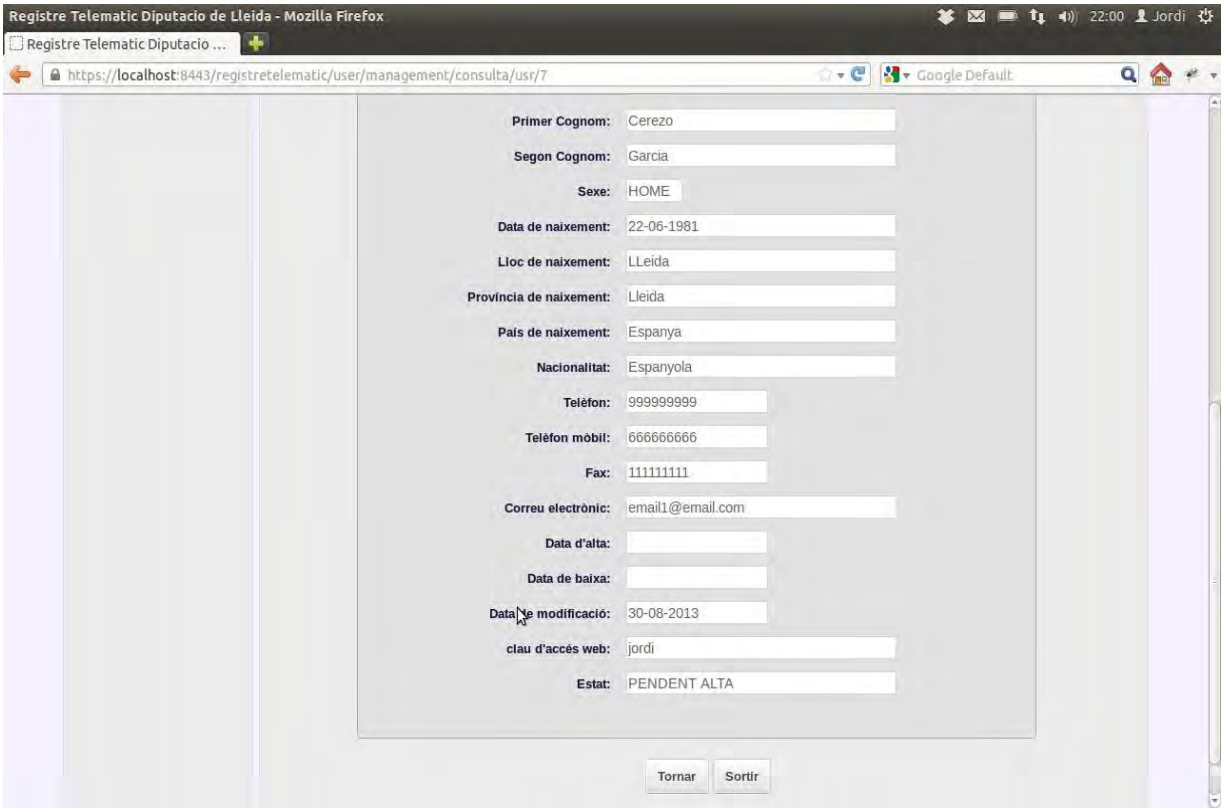
Il·lustració 100: Pantalla de petició de bloqueig del compte web del ciutadà

5.3.3 Gestió de dades personals

La següent entrada del menú lateral fa referència a la gestió de les dades personals de l'usuari que ha iniciat sessió. Es desplegarà un nou menú amb dues opcions.

5.3.3.1 Consulta de dades personals

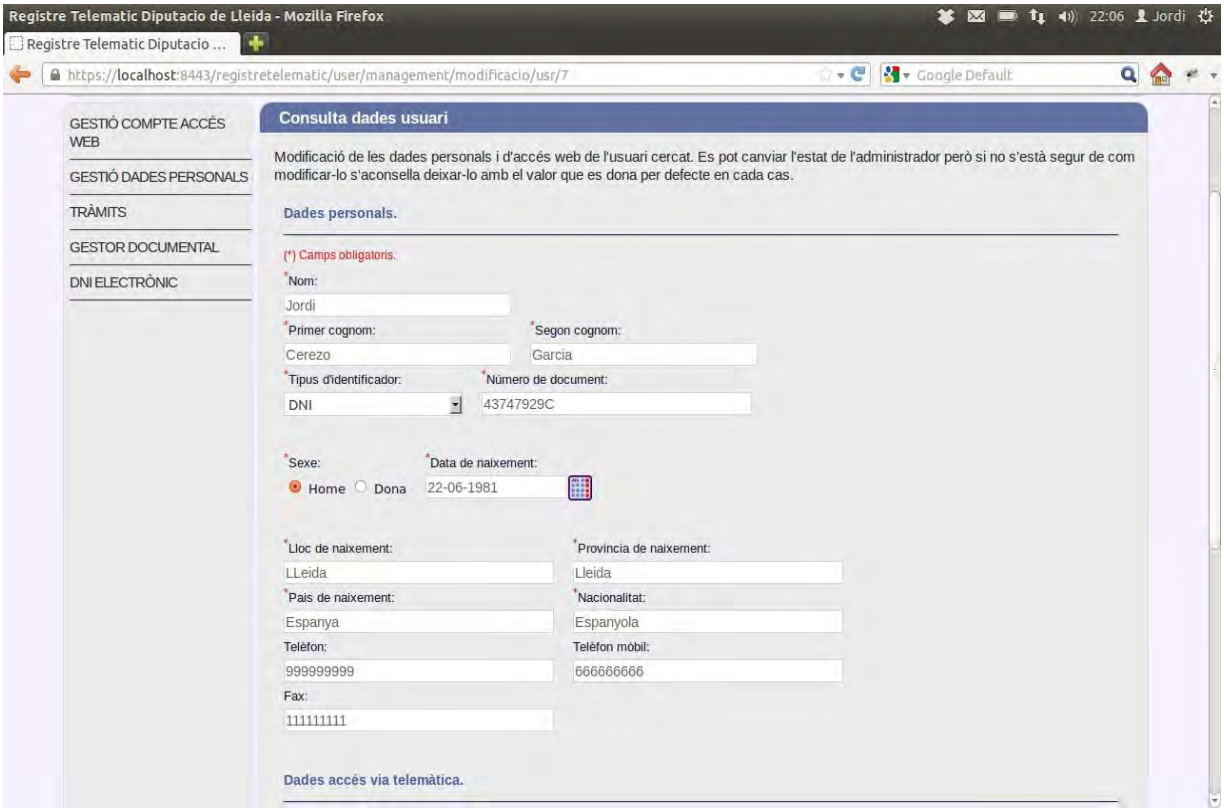
En prémer el botó **"Consulta les teves dades"** una nova finestra apareixerà en pantalla mostrant les dades corresponents a l'usuari connectat a l'aplicació (Il·lustració 101). Les dades d'aquest formulari no poden ser alterades, només consultades (si es volen modificar, consultar l'apartat 5.2.3.4 Modificació usuari). A la part inferior d'aquesta pantalla trobem dos botons. **"Sortir"** ens portarà directament a la pantalla inicial de l'aplicació. **"Tornar"** ens retornarà al cercador de persones, mantenint les opcions de la darrera cerca realitzada.



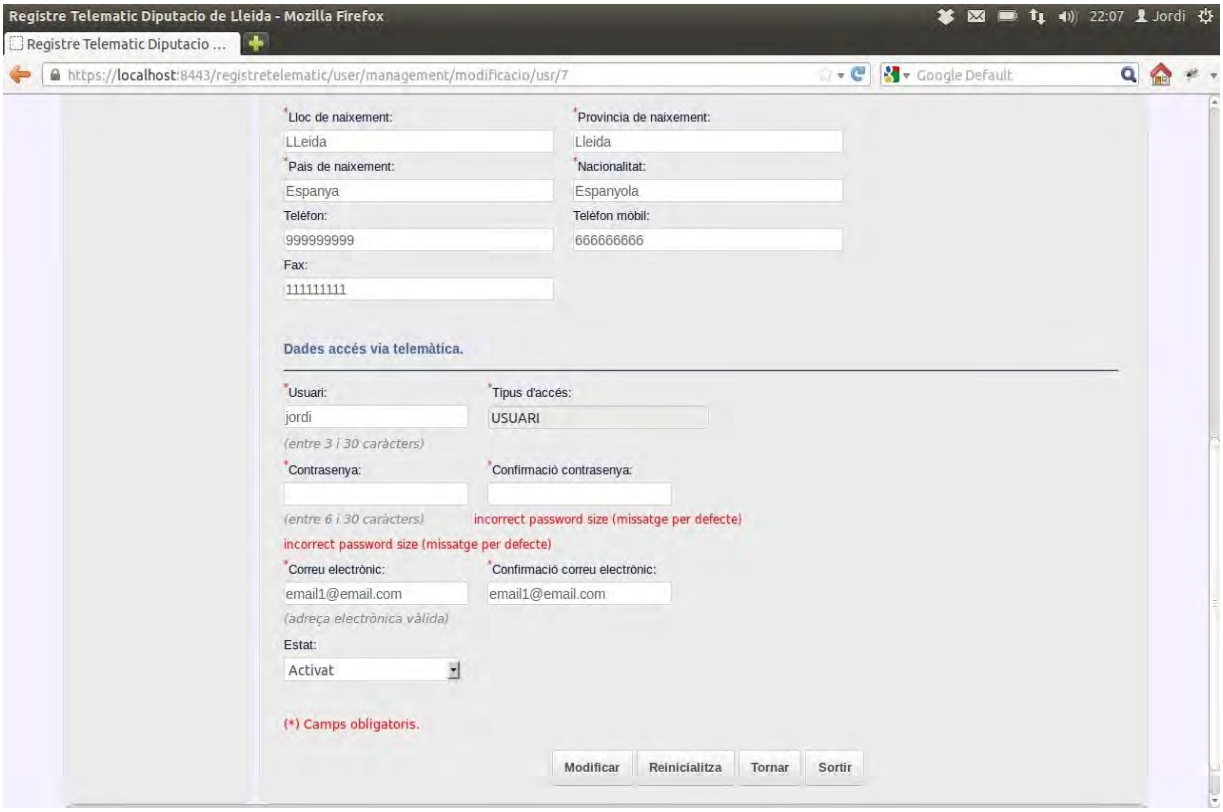
Il·lustració 101: Consulta de les dades d'usuari

5.3.3.2 Modificació de les dades personals

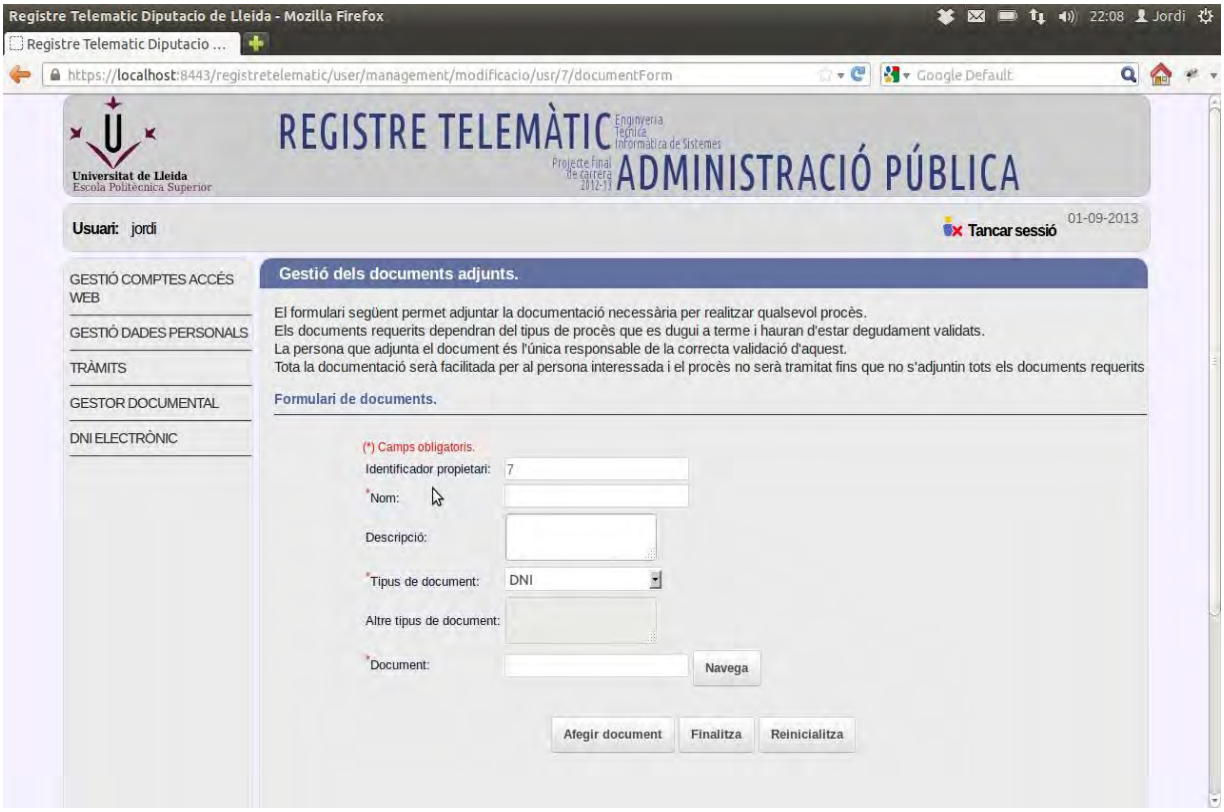
El botó de **"Modificació"** portarà l'usuari a una nova finestra on es mostraran les dades dades corresponents a l'usuari que ha iniciat sessió (Il·lustració 102). A la part inferior d'aquesta pantalla trobem diversos botons. **"Modificar"** servirà per confirmar la modificació de les dades. Si algun dels camps obligatoris queda buit, o bé el tipus de dades introduït no és correcte, apareixerà un missatge a la vora del camp informant de l'error (Il·lustració 103). Si les dades són correctes, el ciutadà serà adreçat a la pantalla d'introducció de documents associats a l'usuari connectat a l'aplicació, per tal d'emmagatzemar còpies dels documents que acrediten les dades proporcionades (Il·lustració 104) (la funcionalitat de **"Gestor documental"** serà tractada en profunditat més endavant en aquest manual). **"Reinicialitza"** posarà totes les dades de l'usuari en blanc. **"Tornar"** ens retornarà al cercador de persones, mantenint les opcions de la darrera cerca realitzada. "**Sortir"** ens portarà directament a la pantalla inicial de l'aplicació.



Il·lustració 102: Modificació dades d'usuari



Il·lustració 103: Error a la modificació d'usuari



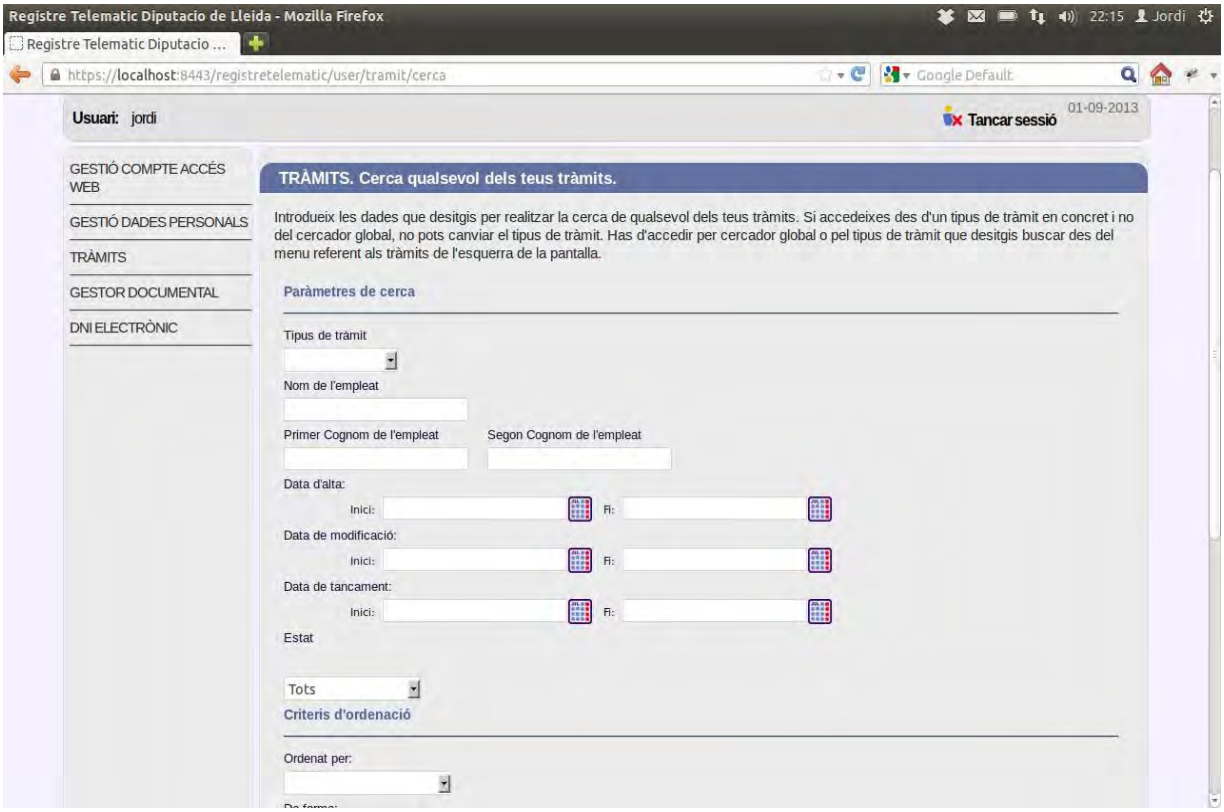
Il·lustració 104: Modificació d'usuari correcta, accés a inserció de documents

5.3.4 Tràmits

L'entrada de menú **"Tràmits"** porta al ciutadà a tots els procediments relacionats amb els diferents tràmits que gestiona l'aplicació. En primer lloc, comentarem el botó que apareix en la posició inferior, **"Cercar qualsevol tràmit"**. Aquest cercador permetrà a l'usuari realitzar una cerca entre tots els tràmits presents a l'aplicació sense distinció de tipus, i que pertanyen a l'usuari connectat a l'aplicació web. La resta de botons mostren les entrades de cadascun dels tipus de tràmits. L'usuari podrà fer cerques acotades només a un tipus de tràmits determinat segons la seva elecció, modificar les seves característiques, i donar d'alta i de baixa de la base de dades els tràmits que seleccionem. Passem a analitzar de forma més acurada cadascun dels botons.

5.3.4.1 Cercar qualsevol tràmit

El botó **"Cerca qualsevol tràmit teu"** portarà l'usuari a una pàgina dedicada a la cerca dels seus tràmits a la base de dades (Il·lustració 105). Es pot considerar una cerca global dels seus tràmits a la base de dades de l'aplicació, ja que no s'està tenint en compte quin tipus de tràmits és el que estem cercant. Aquestes seran les variables del cercador:



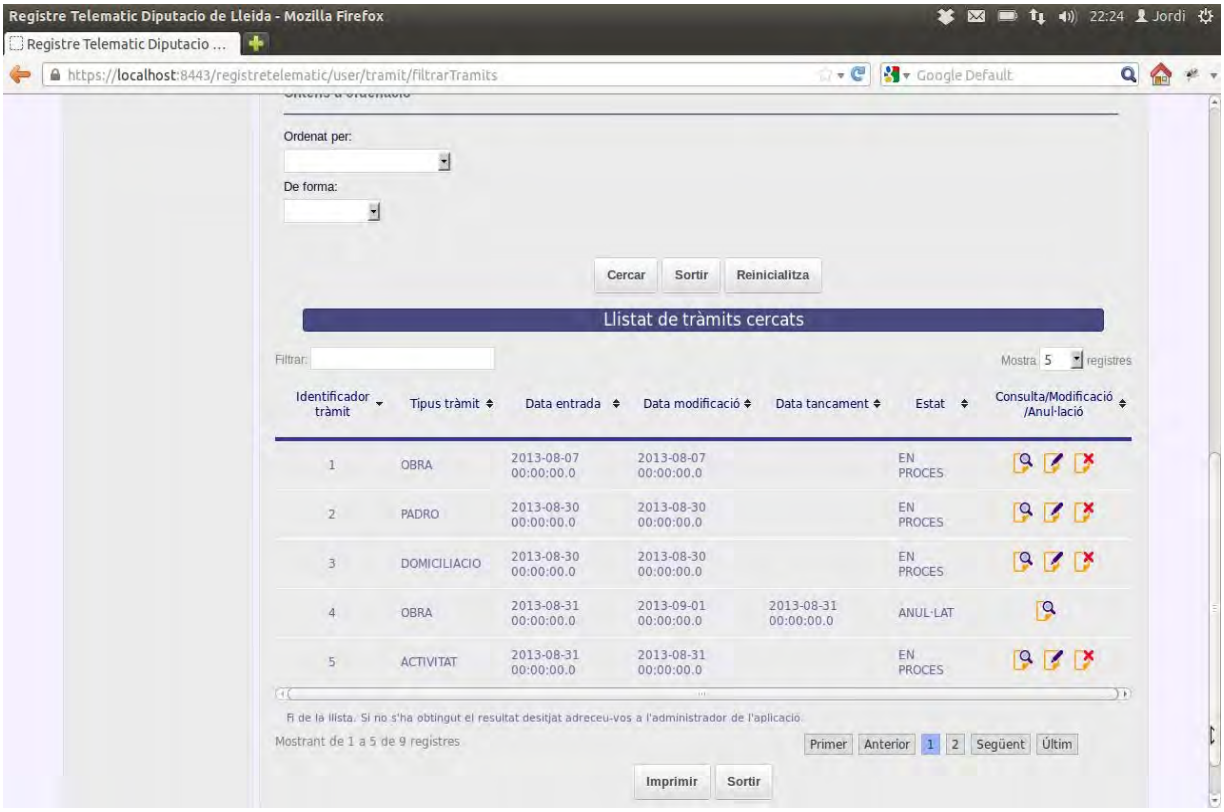
Il·lustració 105: Cercador de tràmits global de l'usuari

- **Tipus de tràmit**: a la part superior de la pàgina es troba un desplegable on es permet triar el tipus de tràmit que s'està cercant. Si no se'n tria cap, la cerca a la base de dades comprendrà tots els tipus de tràmits presents a l'aplicació.
- **Nom, primer cognom i segon cognom de l'empleat**: aquest camps es refereixen al nom complet de l'empleat que ha editat el tràmit o tràmits cercats. Si el ciutadà coneix el nom de l'empleat que l'ha atès, pot emprar aquesta informació per a la cerca entre els seus tràmits. El nom es cercarà comprovant l'existència de la cadena introduïda dins de les dades emmagatzemades als respectius camps a la base de dades. Si els camps es deixen en blanc, no es tindran en compte a l'hora de fer el filtre a la base de dades.
- **Dates**: aquests camps fan referència a les dates d'alta, darrera modificació i tancament respectivament, dels diferents tràmits de la base de dades. La cerca retornarà els tràmits compresos entre les dates d'inici i fi que s'omplin al cercador. Si només s'omple la data d'inici, es cercaran els tràmits amb data posterior a la data introduïda, i fins a l'actualitat. Si, en canvi, s'omple només la data de fi, es cercaran només aquells tràmits amb data anterior a la introduïda. Si els camps es deixen en blanc, no es tindran aquestes dates en compte a l'hora de realitzar la cerca. Per tant, no es filtraran els tràmits segons la seva antiguitat.
- **Estat**: aquest camp fa referència a l'estat del tràmit a la base de dades. Es tracta d'un desplegable que permetrà seleccionar si es volen mostrar els tràmits “Oberts”, “En procés”, “Tancats”, “En Revisió”, o “Anul·lats”. Si es deixa el camp en blanc, no es tindrà en compte aquest criteri a l'hora de realitzar la cerca, per tant es mostraran els tràmits amb qualsevol estat que trobin a la base de dades.
- **Criteris d'ordenació. Ordenat per i De forma**: els criteris d'ordenació fan referència a la

forma en que es vol que ens aparegui ordenada la llista de tràmits que ens retornarà la cerca a la base de dades. “Ordenat per” es refereix al camp pel qual volem ordenar. És a dir, si es tria el nom d'usuari, la taula de resultats ens apareixerà ordenada alfabèticament segons el nom d'usuari. Si es tria una data, estarà ordenada segons l'antiguitat d'aquella data. El criteri “De forma” fa referència al mètode d'ordenament. Si es tria ascendent, una cerca alfabètica serà mostrada des de la “A” fins a la “Z”. Una cerca per data serà mostrada dels registres més antics al més nous. Si, en canvi, es marca l'opció descendent, l'ordenació alfabètica serà inversa, i la cerca per antiguitat anirà del tràmit més nou al més antic dels que formen part de la llista de tràmits cercats. Si es deixen en blancs aquests camps, la taula mostrarà el llistat de tràmits segons l'ordre en que han estat introduïts a la base de dades.

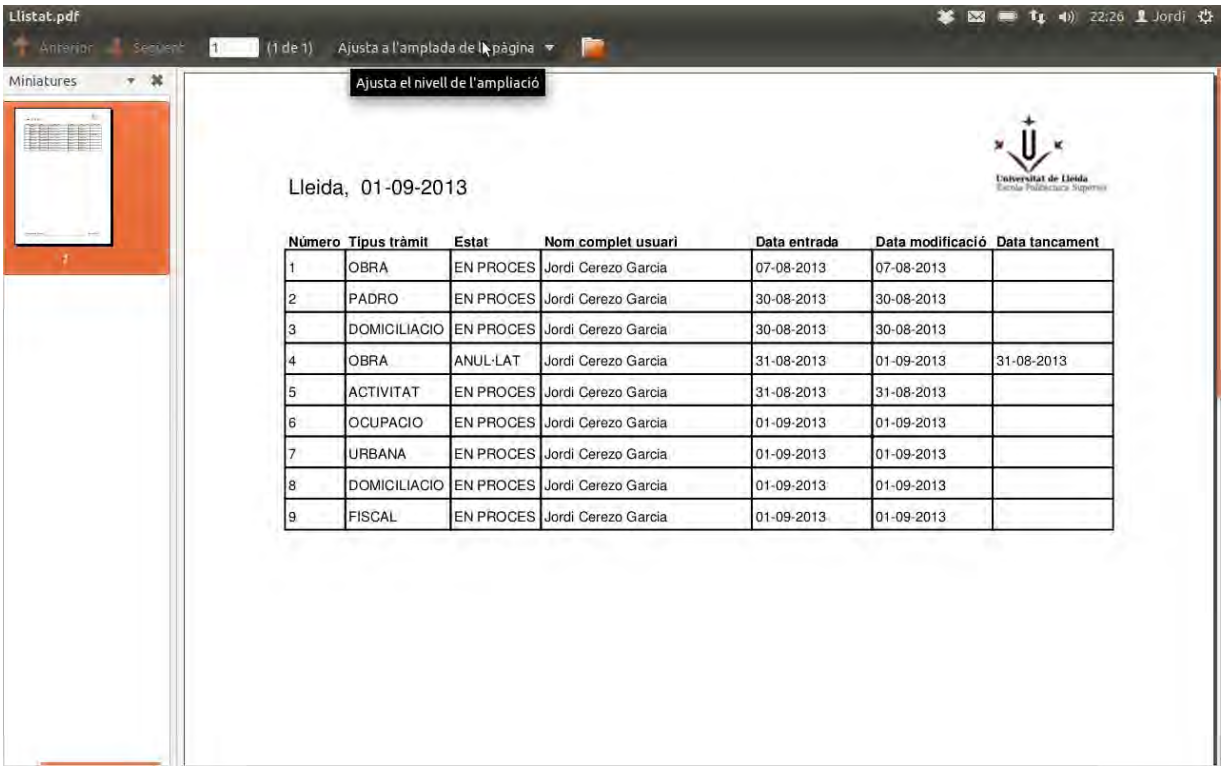
Per realitzar la cerca, s'ha de prémer el botó **“Cercar”**. El botó **“Reinicialitza”** restaura tots els camps del cercador al seu estat per defecte. El botó **“Sortir”** ens porta directament a la pantalla de benvinguda de l'aplicació.

La llista de la part inferior de la pantalla contindrà, com s'ha esmentat anteriorment, els resultats de la la darrera cerca realitzada (Il·lustració 106). Aquesta taula té diverses funcionalitats pròpies. A la part superior esquerra hi ha una caixa de text mitjançant la qual es poden filtrar els resultats de la taula, amb a finalitat d'afinar encara més la cerca. A la part superior dreta es pot introduir el número de registres que es volen mostrar a cada pàgina de la taula. A la part inferior dreta hi ha una sèrie de botons que permeten la navegació a través dels registres de la taula, portant a l'usuari de forma directa a la primera pàgina, la pàgina anterior, la pàgina següent, la pàgina final, i qualsevol d'elles de manera directa, mitjançant el seu número. ***Totes les taules de resultats de l'aplicació tenen la mateixa funcionalitat, per tant, en totes les pantalles que mostrin un llistat d'ara en endavant en aquest document, obviarem l'explicació del funcionament de la taula, i la navegació pels registres mostrats.***



Il·lustració 106: Cerca de tràmits de l'usuari amb llistat de resultats

La taula conté tots els resultats que s'adeqüen a la cerca realitzada. La darrera columna conté tres icones diferents a cada registre de la taula. La primera icona, amb una petita lupa, ens permet realitzar una consulta de les dades del tràmit. La segona icona, amb un petit llapis, ens permetrà realitzar una modificació de les dades del tràmit tractat. La darrera icona, amb una petita creu vermella, permetrà eliminar el registre corresponent, de tal manera que a la base de dades quedarà marcat com a desactivat. A la part inferior del llistat trobem dos botons. El botó **"Imprimir"** permetrà l'usuari crear un document de tipus pdf, amb el llistat de tràmits cercat (Il·lustració 107) i que podrà ser imprès en paper. El botó **"Sortir"** portarà l'empleat a la pàgina inicial de l'aplicació.



Número	Tipus tràmit	Estat	Nom complet usuari	Data entrada	Data modificació	Data tancament
1	OBRA	EN PROCES	Jordi Cerezo Garcia	07-08-2013	07-08-2013	
2	PADRO	EN PROCES	Jordi Cerezo Garcia	30-08-2013	30-08-2013	
3	DOMICILIACIO	EN PROCES	Jordi Cerezo Garcia	30-08-2013	30-08-2013	
4	OBRA	ANUL·LAT	Jordi Cerezo Garcia	31-08-2013	01-09-2013	31-08-2013
5	ACTIVITAT	EN PROCES	Jordi Cerezo Garcia	31-08-2013	31-08-2013	
6	OCUPACIO	EN PROCES	Jordi Cerezo Garcia	01-09-2013	01-09-2013	
7	URBANA	EN PROCES	Jordi Cerezo Garcia	01-09-2013	01-09-2013	
8	DOMICILIACIO	EN PROCES	Jordi Cerezo Garcia	01-09-2013	01-09-2013	
9	FISCAL	EN PROCES	Jordi Cerezo Garcia	01-09-2013	01-09-2013	

Il·lustració 107: Pdf llistat de tràmits cercats de l'usuari

5.3.4.2 Gestió de tràmits

Després de la cerca, passarem a donar una explicació sobre la gestió dels diferents tipus de tràmits. Les diferents operacions que poden ser realitzades s'agruparan de forma independent al tipus de tràmit tractat, és a dir, una alta, una consulta, una modificació o una anul·lació d'un tràmit, seran iguals sense importar si parlem d'un permís d'obra o d'una llicència d'ús i ocupació. Existeixen petites diferències entre els diferents tipus de tràmits, així q primerament es farà una petita introducció als tràmits presents a l'aplicació.

El primer tipus de tràmit que veiem és el "**Padró d'habitants**". Amb aquest tipus de tràmit, una Administració pública pot emmagatzemar totes les dades referents als seus ciutadans, i realitzar un recompte en moments en que sigui necessari. S'ha de tenir en compte en el tràmit de tipus **"Padró"**, que, per a un ciutadà en particular, només pot existir un **"Padró" actiu**, i així quedarà reflectit a la base de dades. La resta de padrons inactius, es conservaran a la base de dades, a mode d'històric per als empleats de l'Administració Pública, per tal de saber les diferents residències per les que ha passat un ciutadà, però no seran accessibles per al propi ciutadà. Aquest, només tindrà accés al seu **"Padró" actiu**.

El segon tipus de tràmit que trobem a l'aplicació és el **"Permís d'obra"**. Aquest tràmit permet a un ciutadà sol·licitar a l'Administració el permís pertinent per dur a terme una obra en un immoble de la seva propietat. Quan disposi d'ell, podrà realitzar l'edificació, adequació o reforma de l'immoble. En aquest tràmit s'ha de remarcar l'existència de dues adreces diferents entre les dades que hi fan referència. El domicili del permís d'obra fa referència a l'adreça on està ubicat l'edifici on es realitzarà l'obra. El domicili de notificació fa referència a l'adreça on s'enviaran les notificacions referents al tràmit.

El tràmit **"Llicència d'Activitat"** permet a un ciutadà demanar a l'Administració una autorització per tal de realitzar activitats que poden suposar una incidència ambiental. Per tal de tenir un control sobre les possibles incidències que es puguin ocasionar al medi ambient, com ara la crema de rastrolls o el possible abocament de diverses substàncies a cursos de rius, l'Administració requereix a qualsevol ciutadà que fiqui en el seu coneixement aquestes activitats, per tal de poder realitzar les tasques de neteja o reparació en cas que es produeixi un abocament indegut o qualsevol altra incidència, i depurar responsabilitat davant greus atacs cap al medi ambient.

El tràmit **"Llicència d'Ús i Ocupació"** permet a un ciutadà la comunicació prèvia a l'Administració Pública de la primera utilització i ocupació d'edificis i construccions del nucli urbà. D'aquesta manera, l'Administració té un coneixement sobre quins dels edificis de la ciutat estan habitats i quins no, dada necessària per tal de gestionar els habitatges de la ciutat, i controlar la seva habitabilitat en benefici de la seguretat dels ciutadans.

El següent tràmit que pot ser gestionat a l'aplicació són les **"Sancions de la Guàrdia Urbana"**. Aquest tràmit, com el seu nom indica, permet a l'Administració la introducció i gestió de les sancions imposades per la Guàrdia Urbana de la ciutat. La sanció serà imposada pels agents , i els empleats de l'Administració introduiran la informació a la base de dades de l'aplicació. El ciutadà sancionat podrà introduir les seves dades bancàries per tal de poder realitzar el pagament de la sanció a través de domiciliació bancària, però no podrà donar d'alta noves sancions, com és natural.

La **"Domiciliació de tributs"** és el següent tràmit que trobem a l'aplicació. En aquest cas, un ciutadà pot demanar a l'Administració que tots els pagaments de tributs, o bé algun d'ells de forma específica, pugui ser abonat a través de domiciliació bancària, aportant a l'Administració un número de compte bancari. Existeix la possibilitat de domiciliar els tribut en diversos comptes bancaris, creant diferents registres i marcant els tributs desitjats a cadascun d'ells per separat.

El darrer tràmit present a l'aplicació és l'**“Adreça Fiscal i/o de notificacions”**. L'Administració dona la possibilitat als ciutadans i empreses de la seva circumscripció d'aportar una adreça fiscal per tal de realitzar les tasques a nivell fiscal, o una adreça de notificacions per tal de mantenir informat al ciutadà de tot allò que li pot resultar necessari en quant a la seva activitat fiscal.

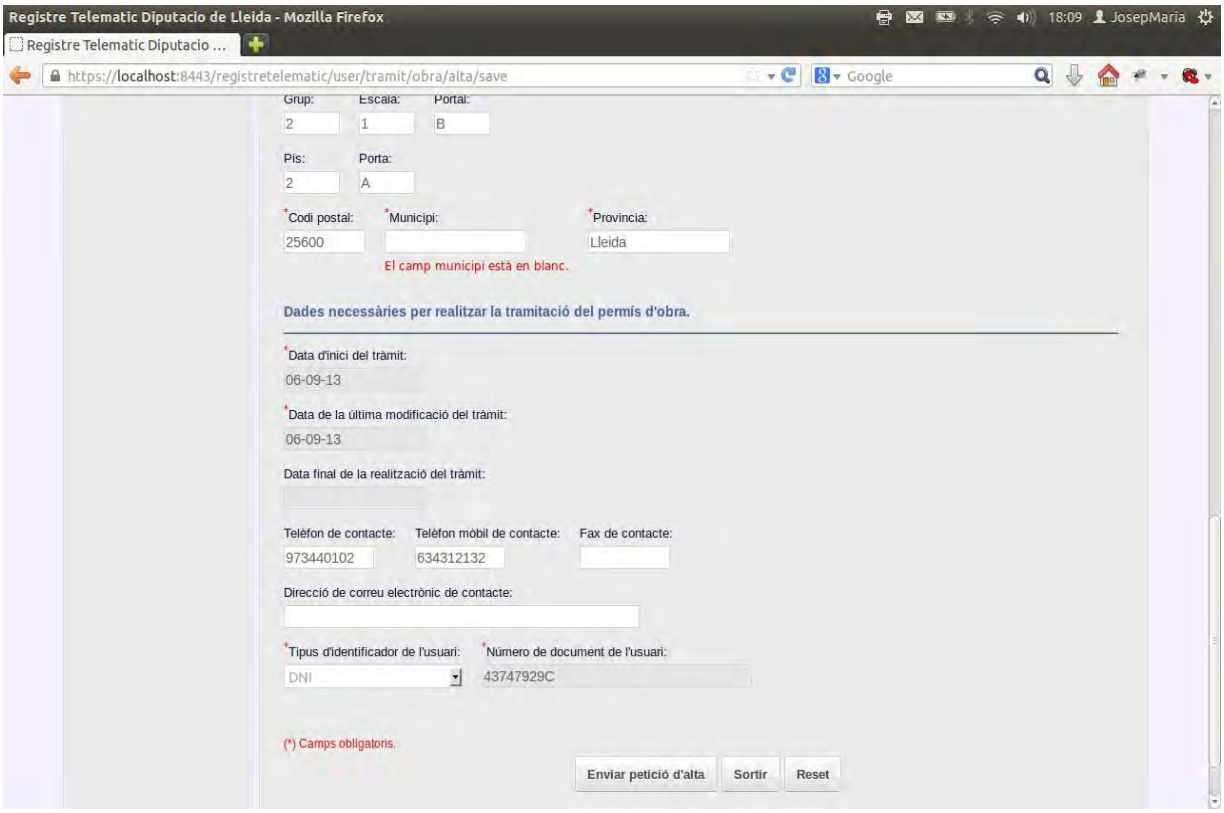
En quant als tràmits que s'emmagatzemen a l'aplicació, és important fer un incís sobre els possibles estats en que es poden trobar els diferents registres. Aquests estats són els següents:

- **Obert**: aquest serà l'estat inicial en que quedarà un tràmit quan és creat per un ciutadà. Haurà de ser comprovat per un empleat de l'Administració Pública, que el validarà i donarà el vist-i-plau en cas de ser correcte. Mentre l'empleat no validi el tràmit, es trobarà “en procés”. Un cop validat, passarà a estat “tancat”.
- **En procés**: quan un tràmit que es troba en estat “obert” és consultat per un empleat, aquest tràmit passarà a estar “en procés”. D'aquesta manera es diferencien els tràmits que ja han estat visualitzats per un empleat. Mentre no en doni el vist-i-plau, el tràmit romandrà en aquest estat. Si un ciutadà modifica un tràmit que ja havia passat al nou estat “en procés” per un empleat, aquest tràmit retornarà al seu estat inicial “obert”. Només un empleat tindrà la capacitat de donar un tràmit per tancat.
- **Tancat**: un tràmit passarà a estar tancat quan, després de ser comprovat per un empleat de l'Administració, aquest en dóna el vist-i-plau. Quan un tràmit es troba en aquest estat, el ciutadà només tindrà la capacitat de consultar-lo, però no en podrà modificar les dades. L'empleat podrà modificar-lo, passant a estar “en revisió”.
- **Revisió**: quan un tràmit prèviament tancat per un empleat ha de ser modificat, passarà a estar en estat de “revisió”. Mentre es troba en revisió, l'empleat tindrà la capacitat de tornar-lo a tancar, quedant modificada la seva data de tancament, o bé passar-lo a estat “anul·lat”.
- **Anul·lat**: quan un empleat detecta un tràmit que presenta alguna errada greu, o incoherències o per qualsevol altre motiu que consideri oportú, pot anul·lar el tràmit. L'empleat podrà posar l'estat “anul·lat” a un tràmit sempre que aquest estigui prèviament “en procés” o en “revisió”.
- **Pendent de signar**: aquest serà l'estat en que quedarà un tràmit prèviament signat pel ciutadà, però que un empleat ha modificat per diversos motius. Els tràmits que es troben en aquest estat, hauran de tornar a ser signats per tal d'evitar incoherència de les dades contingudes i la signatura creada originalment.

Passem seguidament a comentar cadascuna de les possibilitats en quant a la gestió dels tràmits de l'aplicació web. Les captures de pantalla correspondran a un únic tipus de tràmit, però aquestes imatges són extrapolables a qualsevol dels altres tipus.

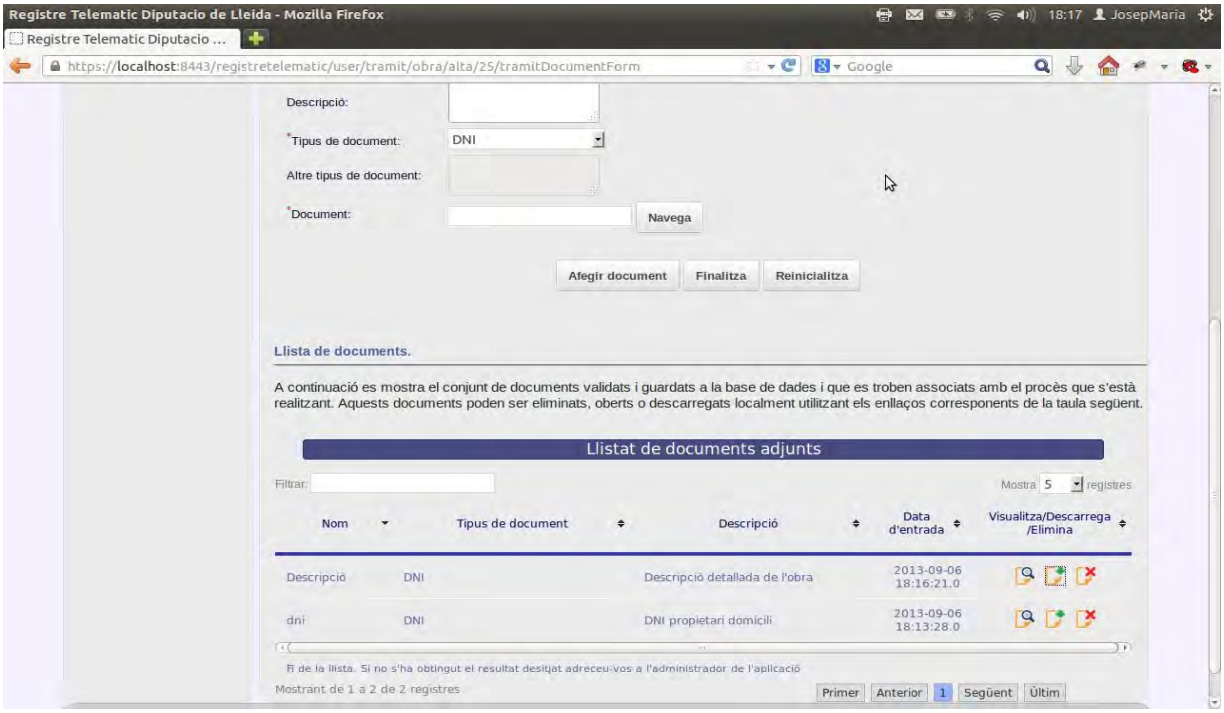
5.3.4.2.1 Alta

L'alta o creació d'un tràmit permet crear un nou registre del tipus de tràmit seleccionat a la base de dades introduint totes les dades necessàries, i que són sol·licitades als diferents formularis d'alta o creació. A la part inferior de la pantalla apareixen diversos botons. **"Sortir"** portarà l'usuari directament a la pantalla de benvinguda de l'aplicació. **"Reset"** reinicialitzarà les dades dels camps del formulari. En prémer el botó **"Enviar petició d'alta",** es farà el procés de signatura, que comentarem posteriorment (5.3.4.2.3 Procés de signatura electrònica d'un tràmit) Si aquest procés es realitza correctament, l'aplicació comprovarà la validesa de les dades introduïdes. En el cas que manqui alguna dada essencial (aquelles que estan marcades amb un asterisc vermell), o algun dels tipus de dades no sigui l'esperat, es marcarà amb missatges d'avís al propi formulari (Il·lustració 108). Quan totes les dades siguin vàlides, es durà a terme l'alta del tràmit a la base de dades.



Il·lustració 108: Alta de tràmit (en aquest cas un permís d'obra) amb error a la introducció de dades

El tràmit creat pertanyerà al ciutadà connectat a l'aplicació. És per aquest motiu que, en aquest formulari, apareixen les dades del document acreditatiu de la identitat del ciutadà, però completades automàticament per l'aplicació, i sense possibilitat de ser modificats.



Il·lustració 109: Gestió de documents associats a un tràmit (en aquest cas un permís d'obra)

Un cop donat d'alta el nou tràmit es mostrarà la finestra de **"Documentació"** (Il·lustració 109). Aquí es dona la oportunitat d'introduir documents referents al tràmit gestionat, en diferents formats per tal de tenir una còpia a la base de dades dels documents oficials que acrediten el tràmit creat, o al propi ciutadà depenent del cas. Els documents s'introdueixen posant el nom i descripció dels mateixos, i un diàleg de sistema operatiu per a cerca de documents a l'equip, permet pujar-lo a la base de dades de l'aplicació. Aquests quedaran reflectits a la taula inferior de la pantalla. Es farà un comentari en profunditat a l'apartat corresponent al gestor documental (5.3.5 Gestor documental).

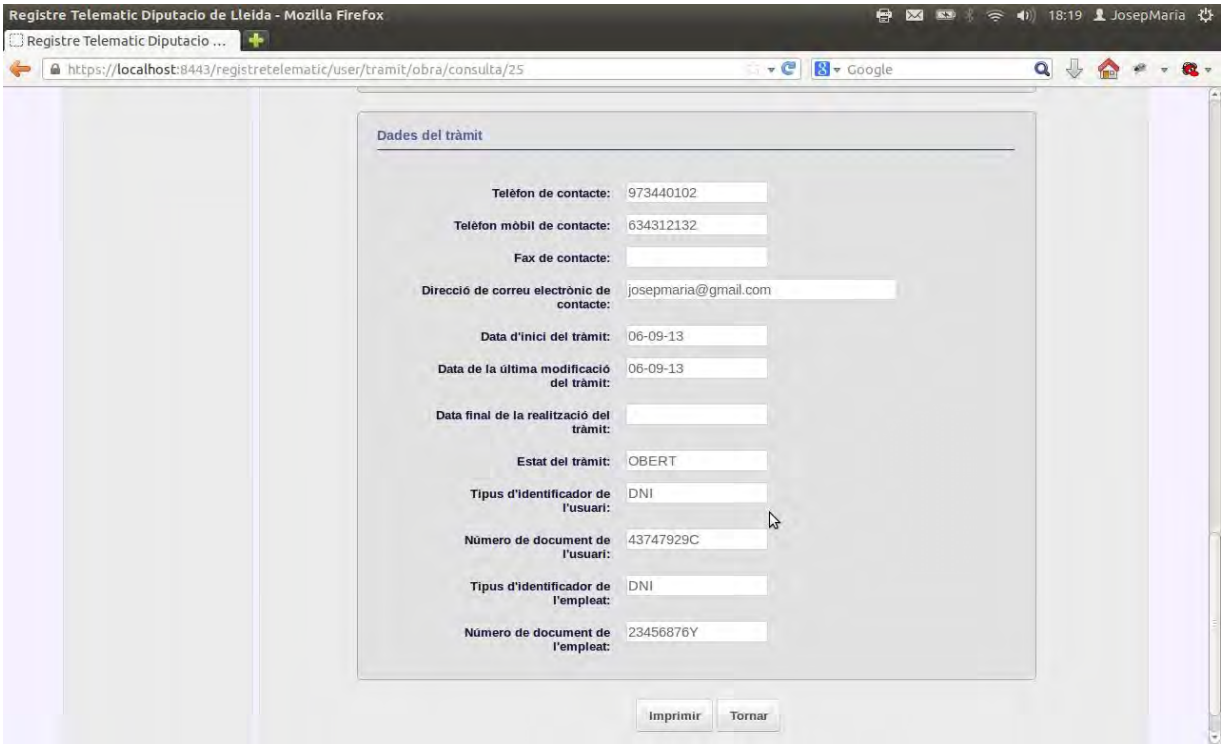
5.3.4.2.2 Consulta, modificació i anul·lació

Els tres botons següents de les entrades de menú de cadascun dels tràmits portaran directament a una **cerca de tràmits** (5.3.4.1 Cercar qualsevol tràmit) amb la particularitat que el tipus de tràmit serà indefectiblement el que s'ha triat a l'entrada de menú. La cerca es realitzarà de la mateixa forma, i amb els mateixos criteris que una cerca global, però el camp **"Tipus Tràmit"** apareixerà en aquest cas deshabilitat, per tal d'assegurar que la cerca es realitza únicament sobre els tràmits del tipus seleccionat. A la part inferior, trobem el botó **"Reinicialitzar",** que tornarà a posar tots els camps del formulari al seu estat inicial i el botó **"Sortir"**, que ens portarà de nou a la pantalla de benvinguda de l'aplicació. Un cop escrits els criteris pels quals es vol realitzar la cerca a la base de dades, s'ha de prémer el botó **"Cercar"**. L'aplicació mostrarà a la taula de la part inferior del formulari, un llistat amb tots els tràmits del tipus seleccionat que compleixen els criteris prèviament seleccionats i que pertanyen a l'usuari connectat a l'aplicació web..

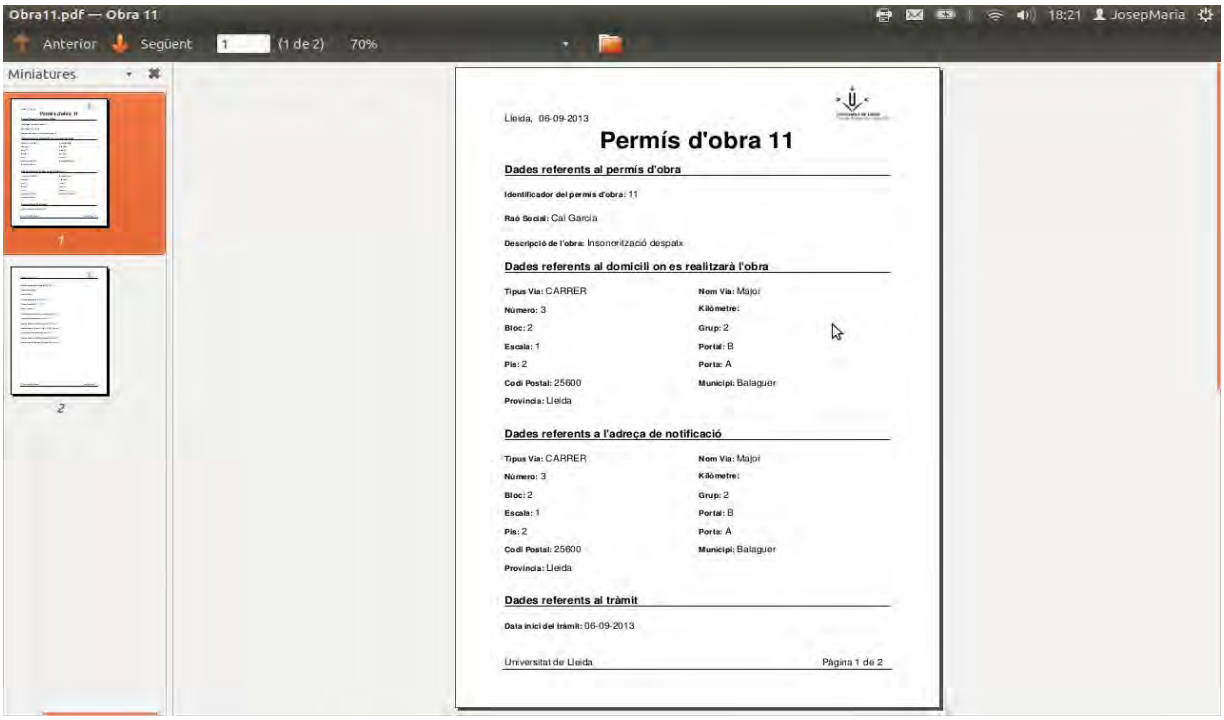
A la darrera de les columnes de la taula de resultats, marcada amb el títol **"Consulta/Modificació/Anul·lació"** apareixen tres icones, que permetran la consulta, modificació i anul·lació del tràmit seleccionat.

La icona de l'esquerra, marcada amb una petita lupa, porta a la pàgina de consulta del registre triat. En aquesta pantalla (Il·lustració 110) es poden consultar totes les dades referents al tràmit, sense possibilitat de modificar-lo. D'aquesta manera tenim la possibilitat de visualitzar les dades

referents al tràmit sense el perill de modificar alguna dada de manera involuntària o accidental. Les dades mostrades en pantalla es poden imprimir en paper mitjançant el botó **"Imprimir"**, que generarà un document pdf que podrà ser obert amb qualsevol programa de visualització de pdf (Il·lustració 111). Un cop consultades les dades, es pot prémer el botó **"Tornar"**, i d'aquesta manera es tornarà al formulari de cerca amb totes les dades de la darrera cerca efectuades en pantalla.

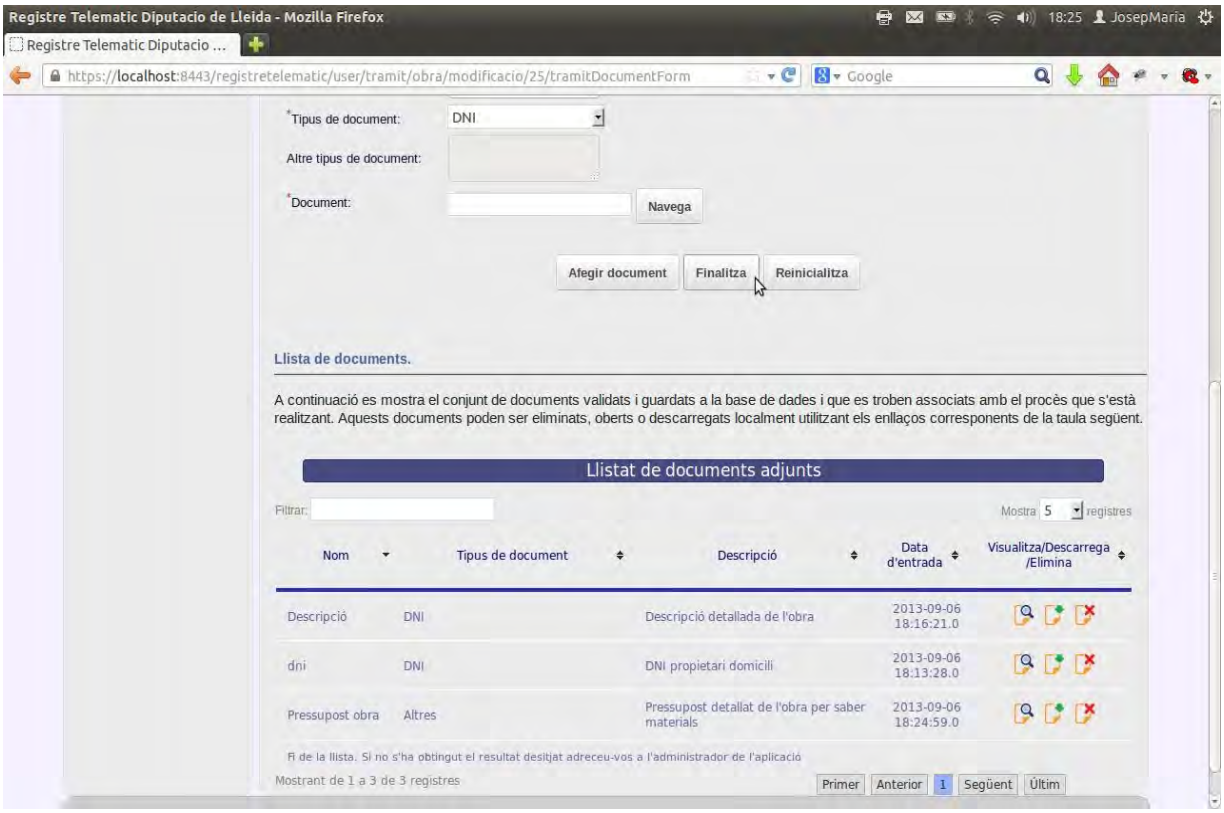


Il·lustració 110: Consulta de tràmit (en aquest cas un permís d'obra), detall de botons inferiors



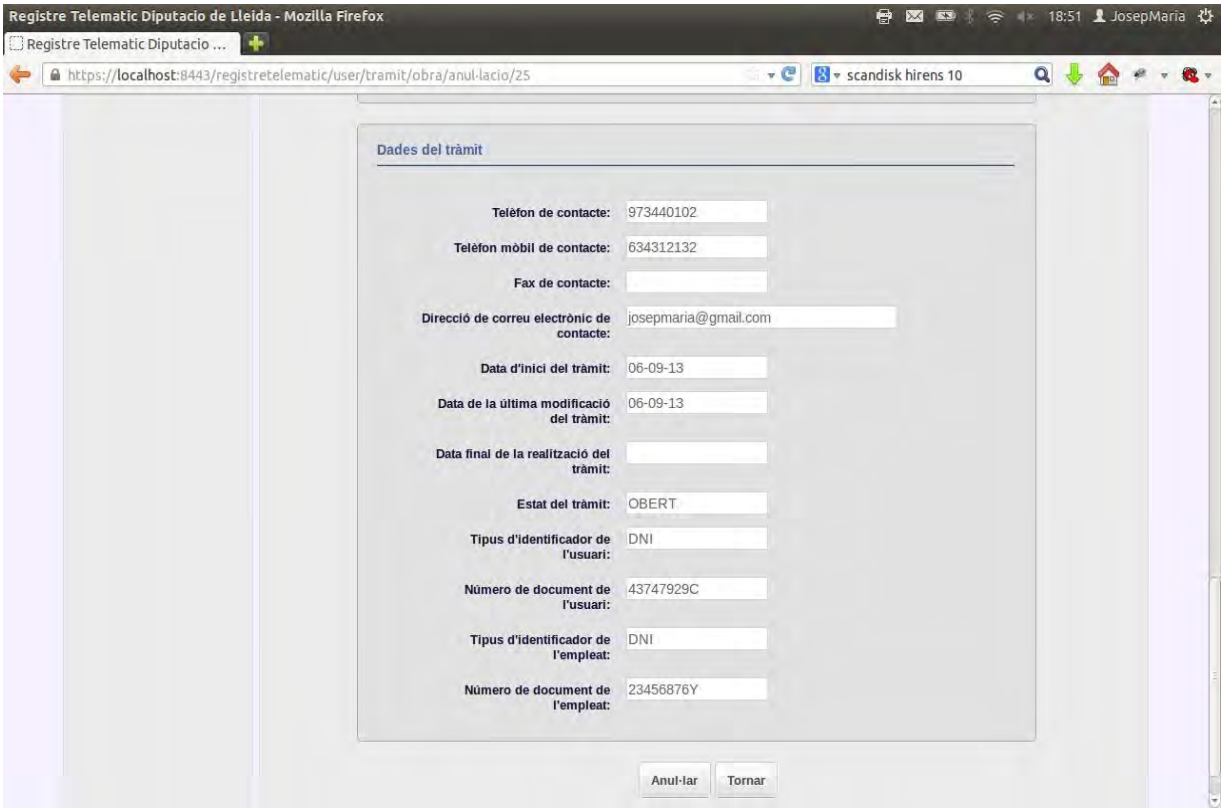
Il·lustració 111: Pdf consulta de tràmit (en aquest cas un permís d'obra)

La icona central de la taula de resultats, la que conté un petit llapis, portarà directament a la pàgina de **modificació del tràmit** escollit. Aquesta pantalla (Il·lustració 112) mostra totes les dades referents al tràmit seleccionat, però en aquest cas les dades sí que es poden modificar. El botó **"Sortir"** portarà directament a la pantalla de benvinguda. El botó **"Reinicialitzar"** buidarà tots els camps del formulari, per tal de tornar a introduir tota la informació de nou. Un cop realitzats els canvis desitjats, s'ha de prémer el botó **"Modificar"**. En aquest punt, es durà a terme el procés de signatura, que comentarem posteriorment (5.3.4.2.3 Procés de signatura electrònica d'un tràmit). Si aquest procés es realitza correctament, l'aplicació comprovarà la validesa de les dades introduïdes. En el cas que alguna dada essencial, les que estan marcades amb un asterisc vermell, no sigui introduïda, o bé el tipus de dada sigui incorrecte, es mostraran els missatges d'error al propi formulari. Un cop les dades siguin vàlides, el tràmit serà introduït a la base de dades, i es passarà a la pantalla d'introducció de documents referents al mateix (Il·lustració 112). Es parlarà en profunditat del gestor documental més endavant en aquest manual (5.3.5 Gestor documental).



Il·lustració 112: Modificació de tràmit (en aquest cas un permís d'obra), detall dels botons

La icona de l'esquerra de la taula de resultats, la que conté una petita creu vermella, portarà directament a la pàgina d'**anul·lació del tràmit** escollit. Aquesta pantalla (Il·lustració 113) mostra totes les dades referents al tràmit seleccionat. En aquest cas les dades no es poden modificar. El botó **"Tornar"** retornarà l'usuari a la pantalla anterior, amb les dades de la darrera cerca que s'ha realitzat. El botó **"Anul·lar"** marcarà aquest tràmit com a anul·lat, i no serà vàlid a l'aplicació. Cal remarcar que el tràmit no serà eliminat de la base de dades, per evitar pèrdues involuntàries d'informació, si no que únicament quedarà marcat amb estat **"ANUL·LAT"**. En anul·lar un tràmit, es mostrarà una pantalla informant que la operació ha estat correcta.

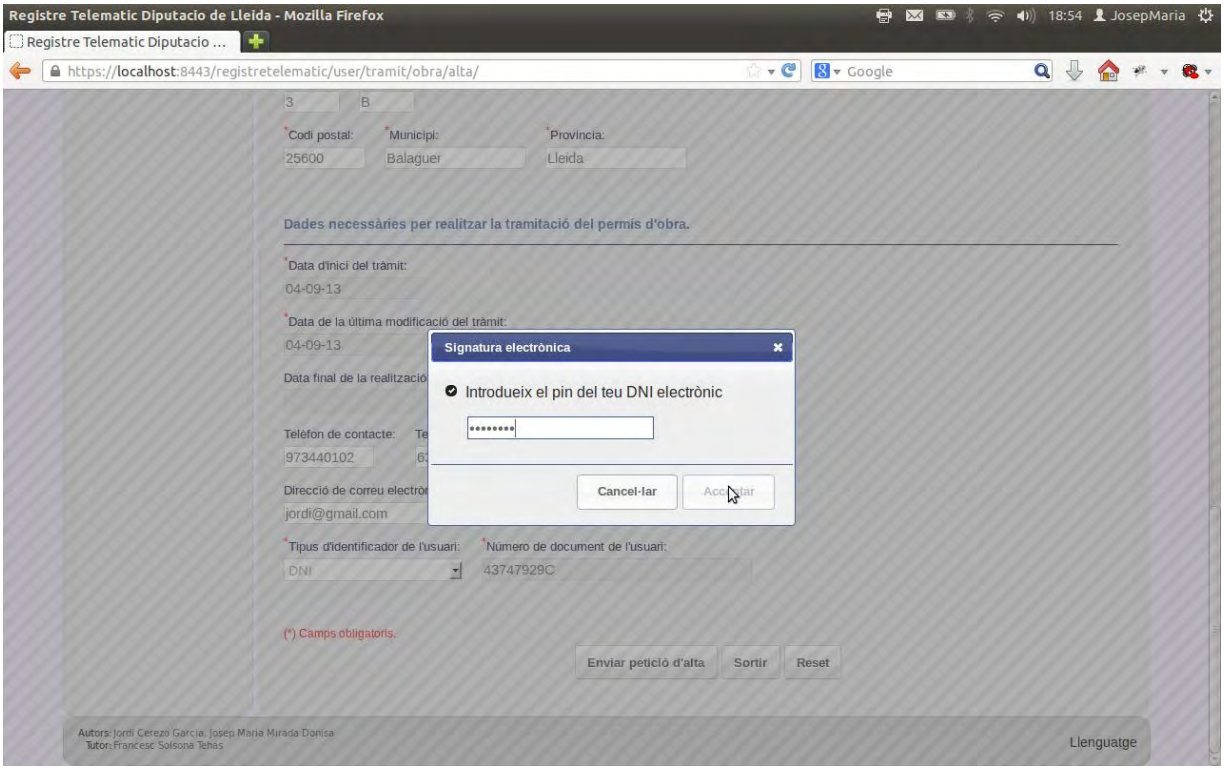


Il·lustració 113: Anul·lació de tràmit (en aquest cas un permís d'obra), detall dels botons

5.3.4.2.3 Procés de signatura electrònica d'un tràmit

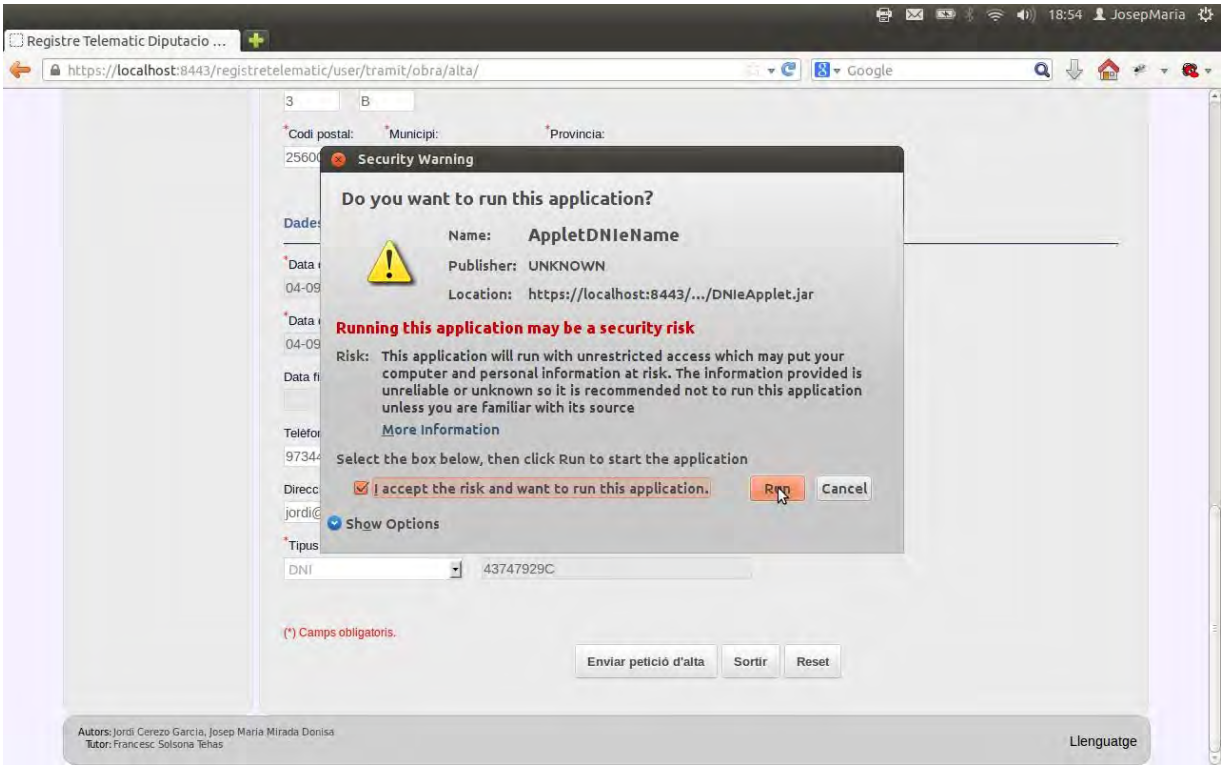
Quan un ciutadà introdueix o modifica un tràmit a la base de dades de l'aplicació web, l'Administració necessita saber de forma inequívoca qui és l'autor de les dades introduïdes al formulari. D'això se'n diu **"autenticació"**. A més, l'Administració necessita tenir la seguretat que el missatge rebut no ha patit cap alteració respecte a les dades que el ciutadà ha introduït originalment, és a dir, s'ha de garantir la **"integritat"** del missatge. Finalment, s'ha de assegurar que la persona que ha completat el formulari no pugui negar la seva autoria un cop hagi enviat les dades, és a dir, s'ha de garantir el **"no repudi"** (2.4.2 Signatura digital).

Totes aquestes necessitats són garantides mitjançant el **DNI-electrònic**. Per això, quan un ciutadà envia una petició d'alta de tràmit, o bé una petició de modificació de dades, l'aplicació web demanarà que aquestes dades siguin signades amb el certificat de signatura contingut al DNI-e. En prémer el botó **"Enviar petició"** al formulari d'alta, o bé el botó **"Modificar"** al de modificació, es mostrarà en pantalla un diàleg demanant el PIN del DNIe (Il·lustració 114).



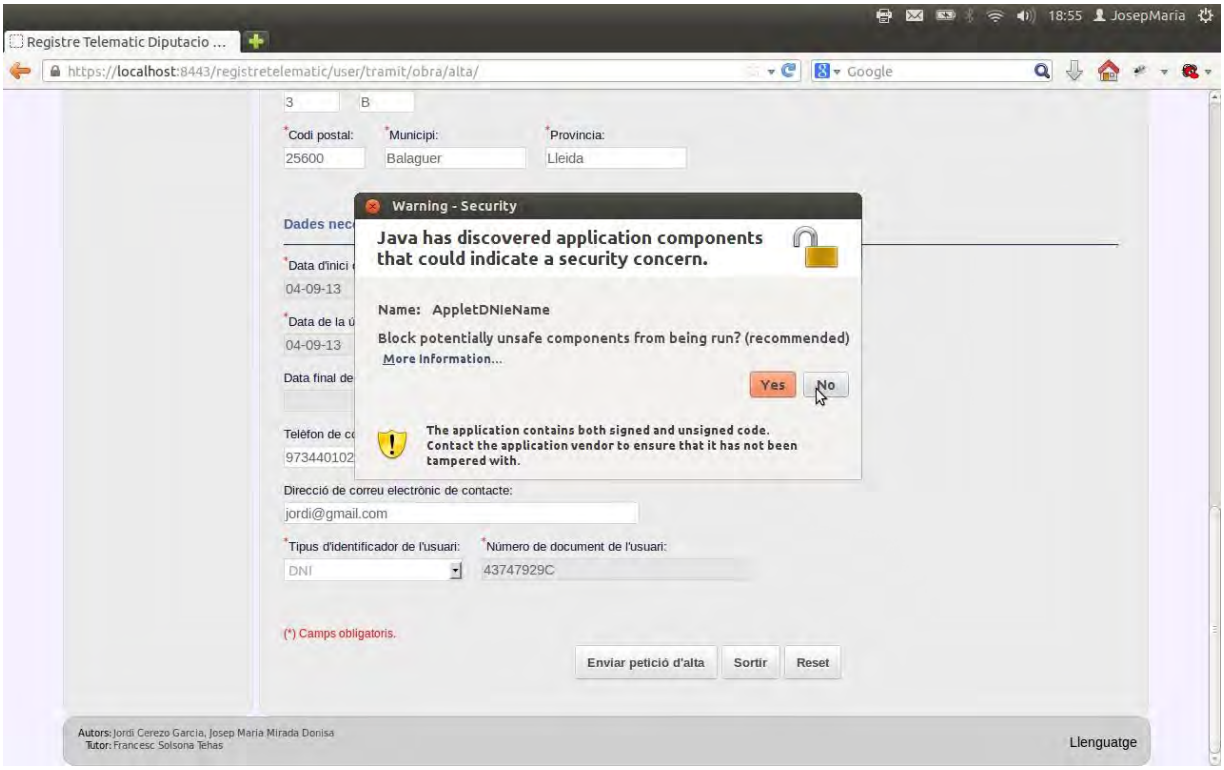
Il·lustració 114: Signatura electrònica. Petició de PIN.

Per motius de seguretat, el plugin de Java demanarà confirmació per a l'execució de l'applet de signatura digital (Il·lustració 115).



Il·lustració 115: Signatura electrònica. Petició de confirmació.

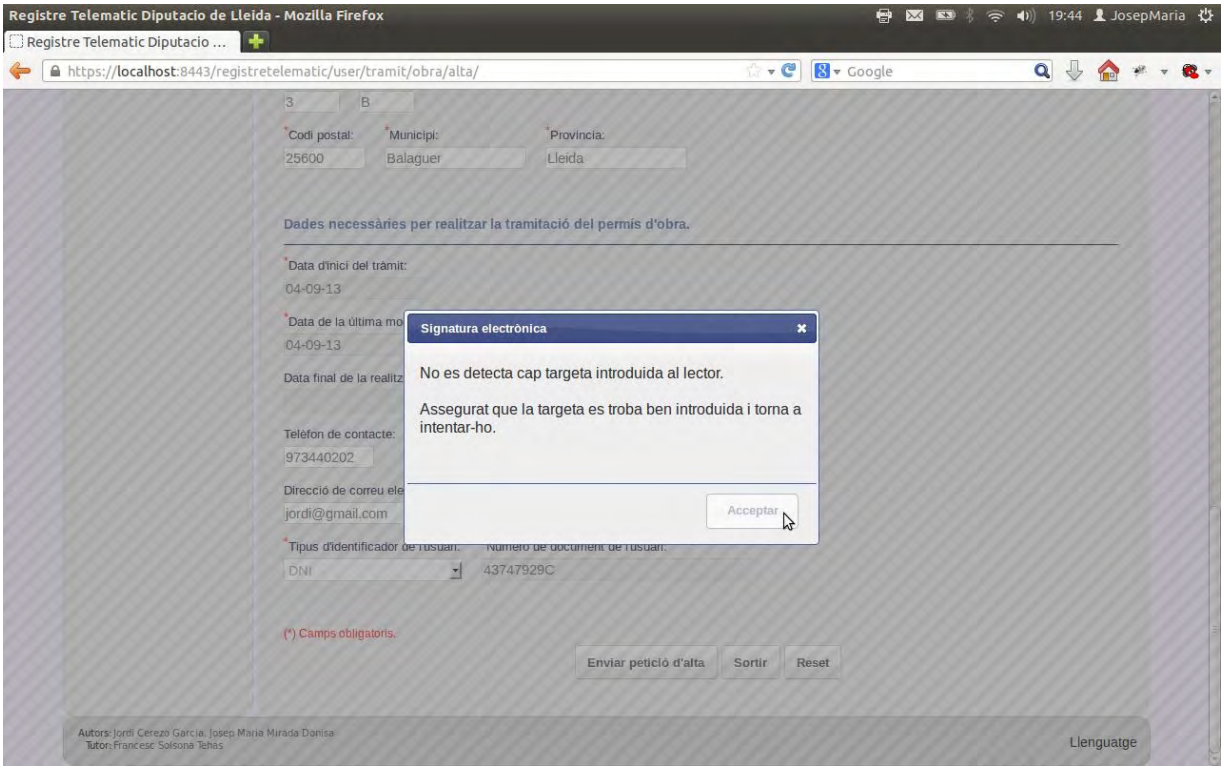
Tot i que el ciutadà doni el seu permís, Java voldrà bloquejar l'execució en segona instància, donat que detecta que el codi és potencialment perillós (Il·lustració 116).



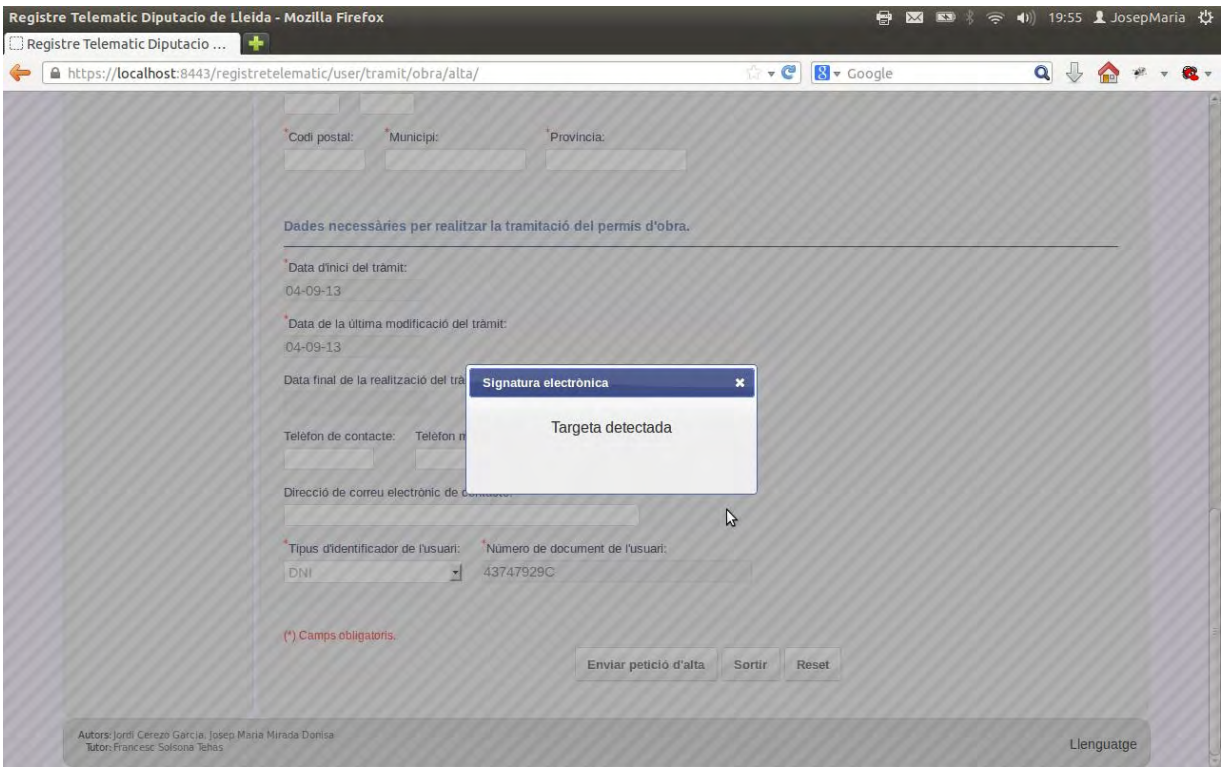
Il·lustració 116: Signatura electrònica. Petició de bloqueig.

En aquest cas, el ciutadà haurà de negar aquest bloqueig, ja que confia en el software posat a la seva disposició per part de l'Administració. El següent pas que fa l'applet és comprovar si hi ha una targeta introduïda realment al lector:

- Si no en troba cap (Il·lustració 117), s'atura l'execució retornant al formulari del tràmit.
- Si hi ha una targeta introduïda (Il·lustració 118), continuarà el procés de signatura.



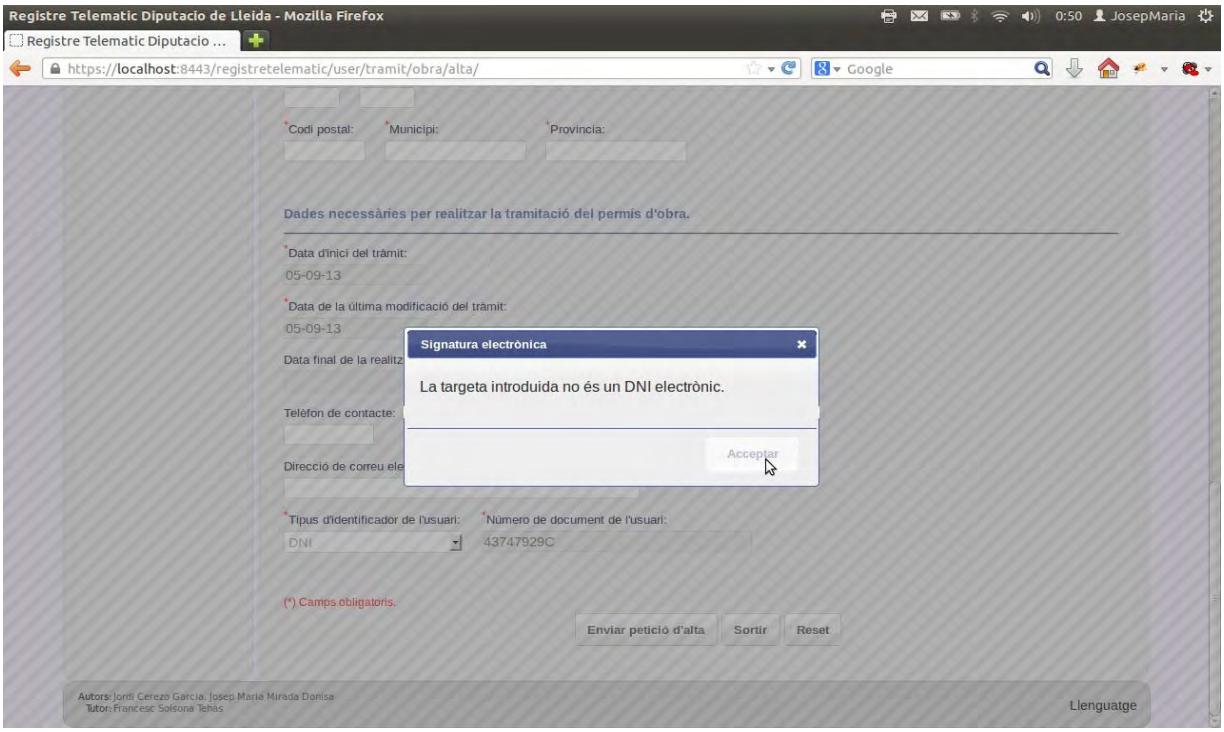
Il·lustració 117: Signatura electrònica. Error de detecció de targeta al lector.



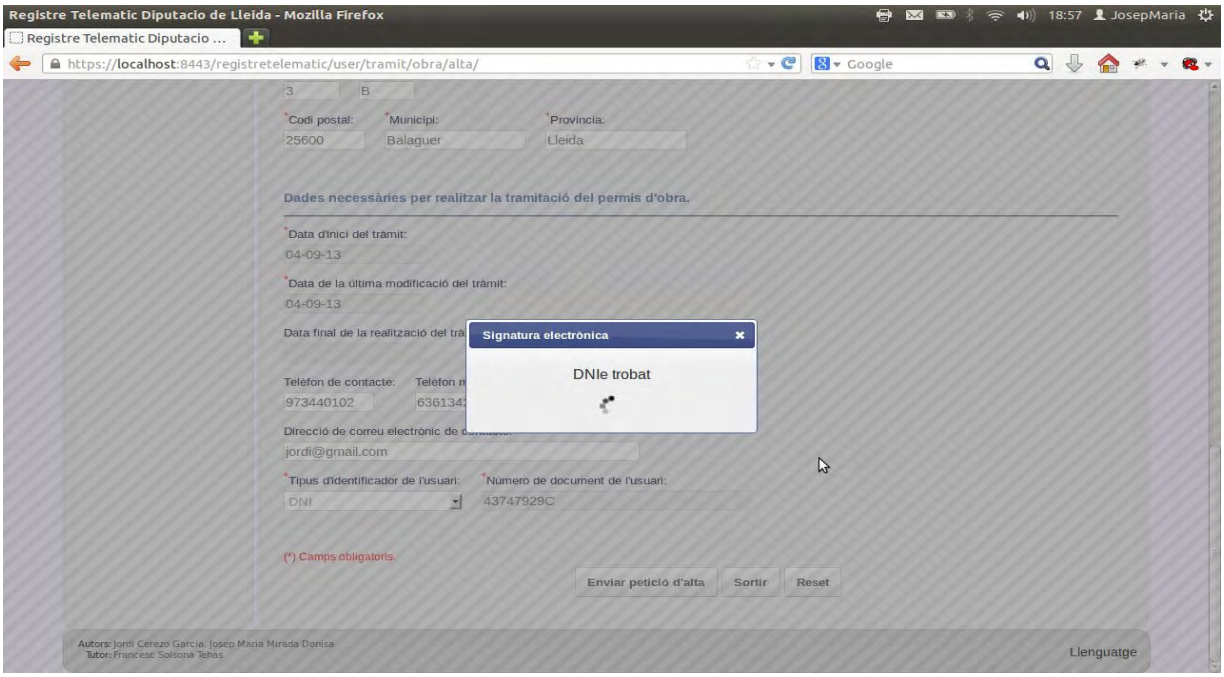
Il·lustració 118: Signatura electrònica. Targeta detectada correctament.

Seguidament, comprovarà si realment la targeta és un DNI-e:

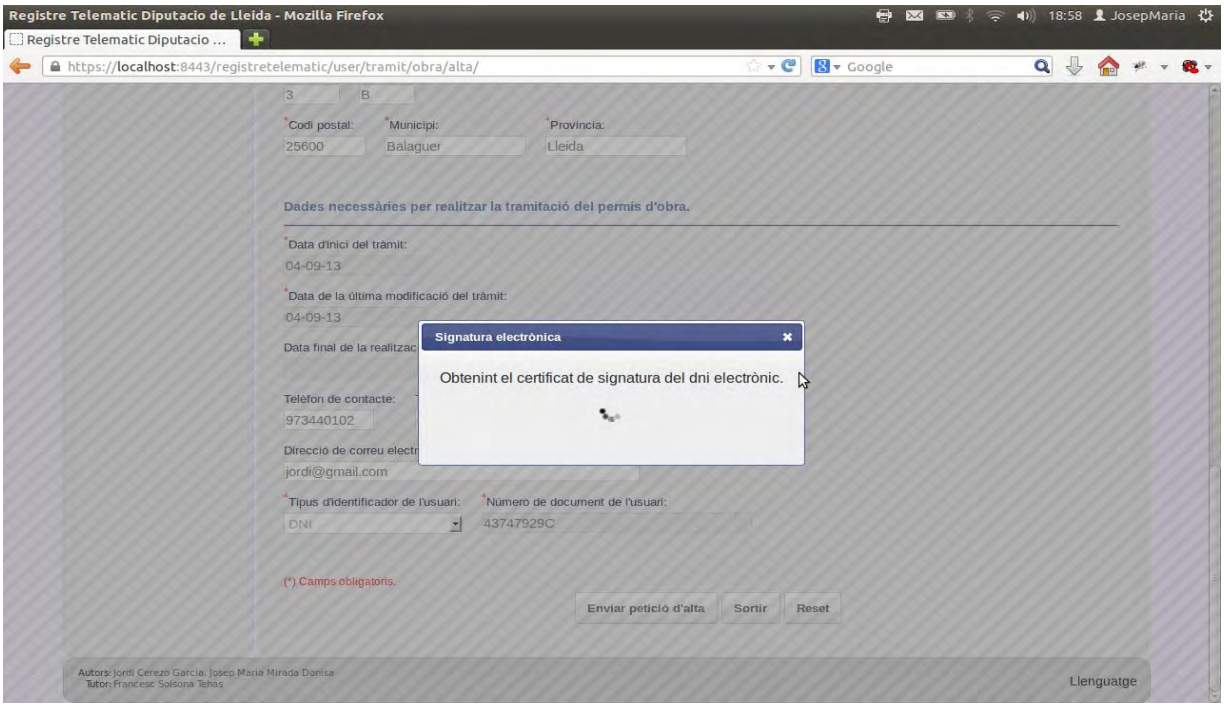
- En el cas que no ho sigui (Il·lustració 119), es mostrarà una pantalla informant al ciutadà de l'error i finalitzarà l'execució de l'applet de signatura, retornant a la pantalla del formulari d'introducció de dades del tràmit.
- En el cas que la targeta sigui, efectivament, un DNIe (Il·lustració 120), s'obtindrà el certificat de signatura que conté (Il·lustració 121).



Il·lustració 119: Signatura electrònica. Error de detecció del DNI-e.



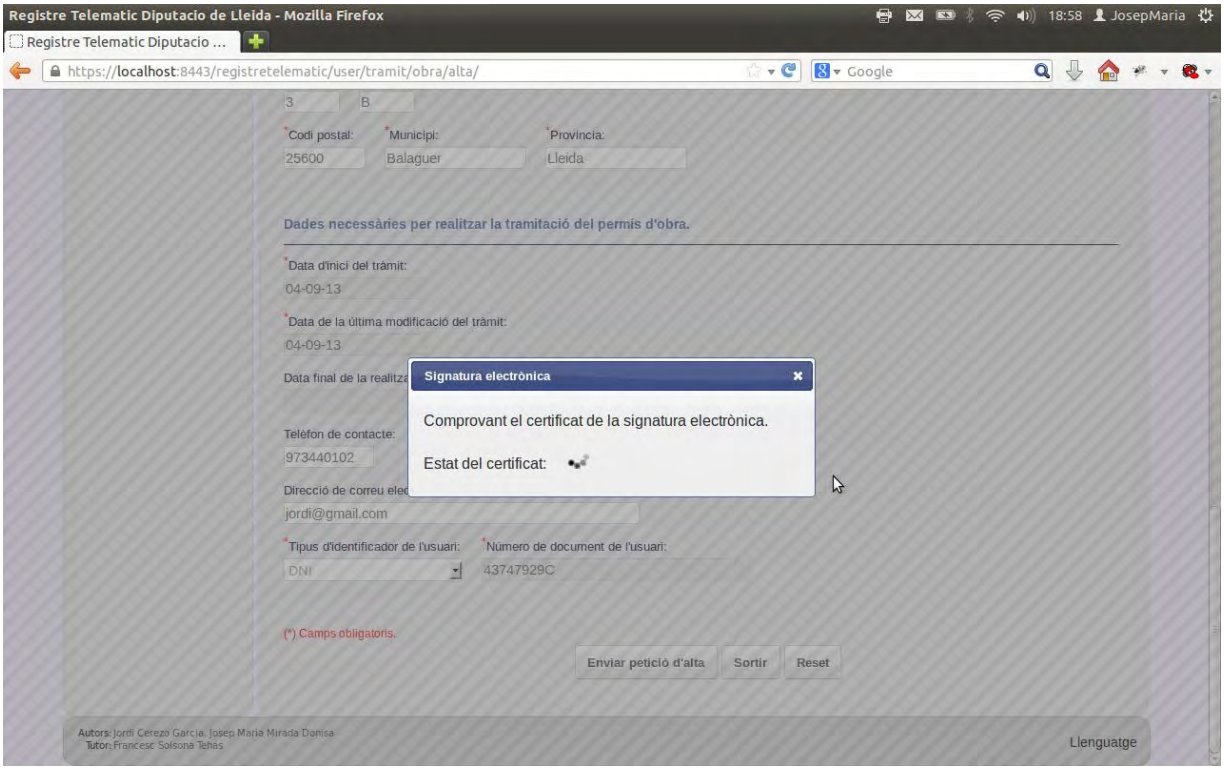
Il·lustració 120: Signatura electrònica. Detecció de DNIe correcta.



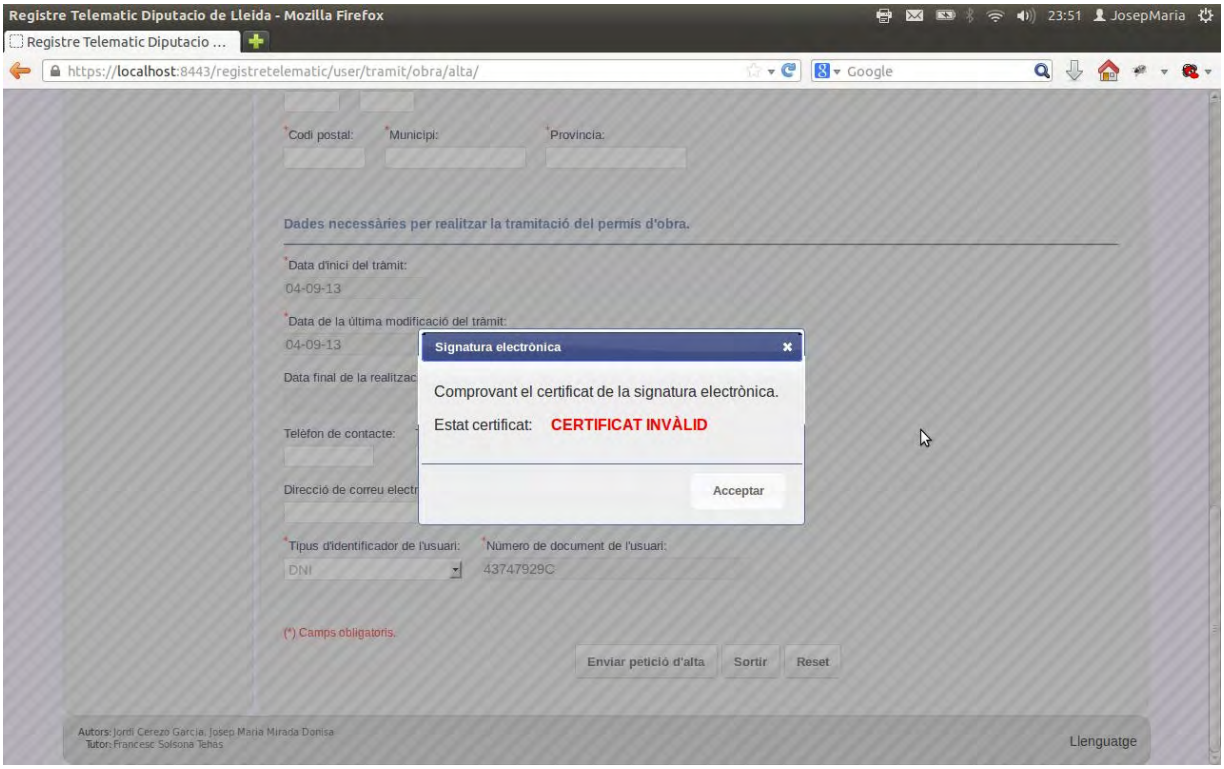
Il·lustració 121: Signatura electrònica. Obtenció de certificat.

Tot seguit, es comprovarà la validesa del certificat de signatura obtingut (Il·lustració 122):

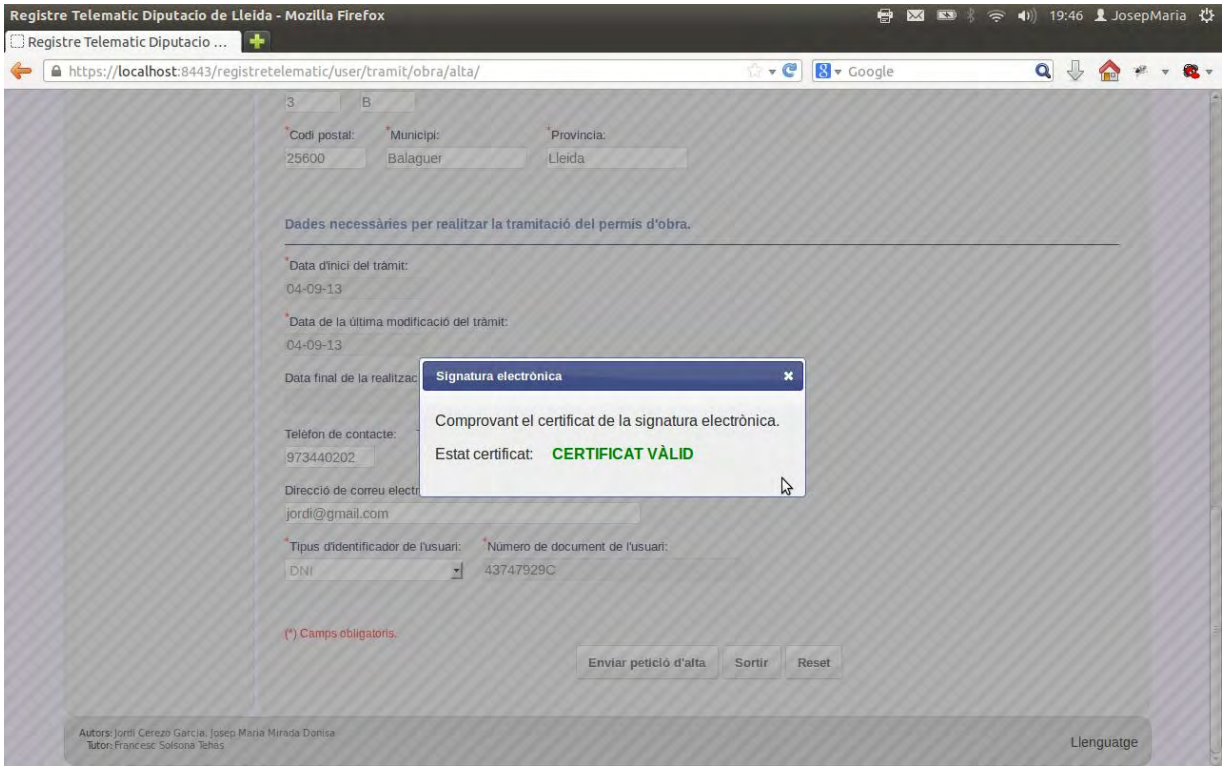
- Si el certificat és invàlid (Il·lustració 123), es finalitzarà l'execució de l'applet, retornant al formulari del tràmit.
- Si, en canvi, el certificat és vàlid (Il·lustració 124), continuarà el procés de signatura.



Il·lustració 122: Signatura electrònica. Certificat obtingut correctament.

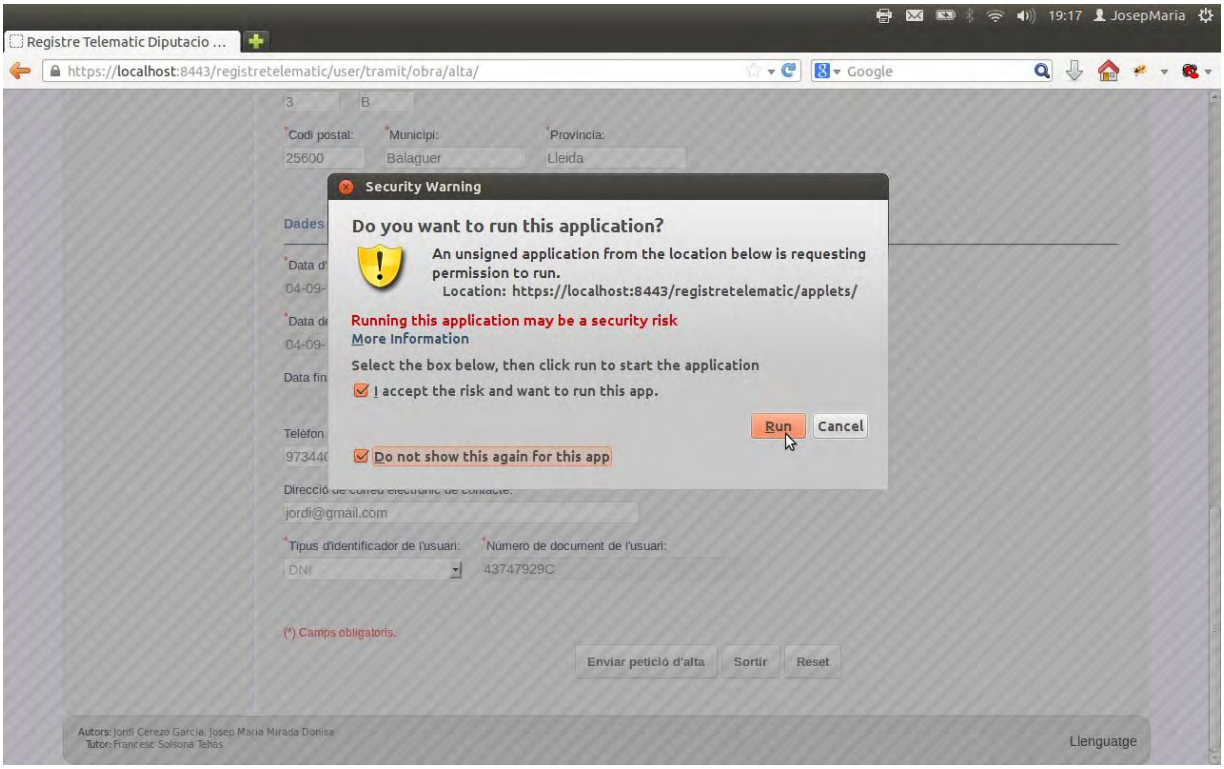


Il·lustració 123: Signatura electrònica. Certificat invàlid.



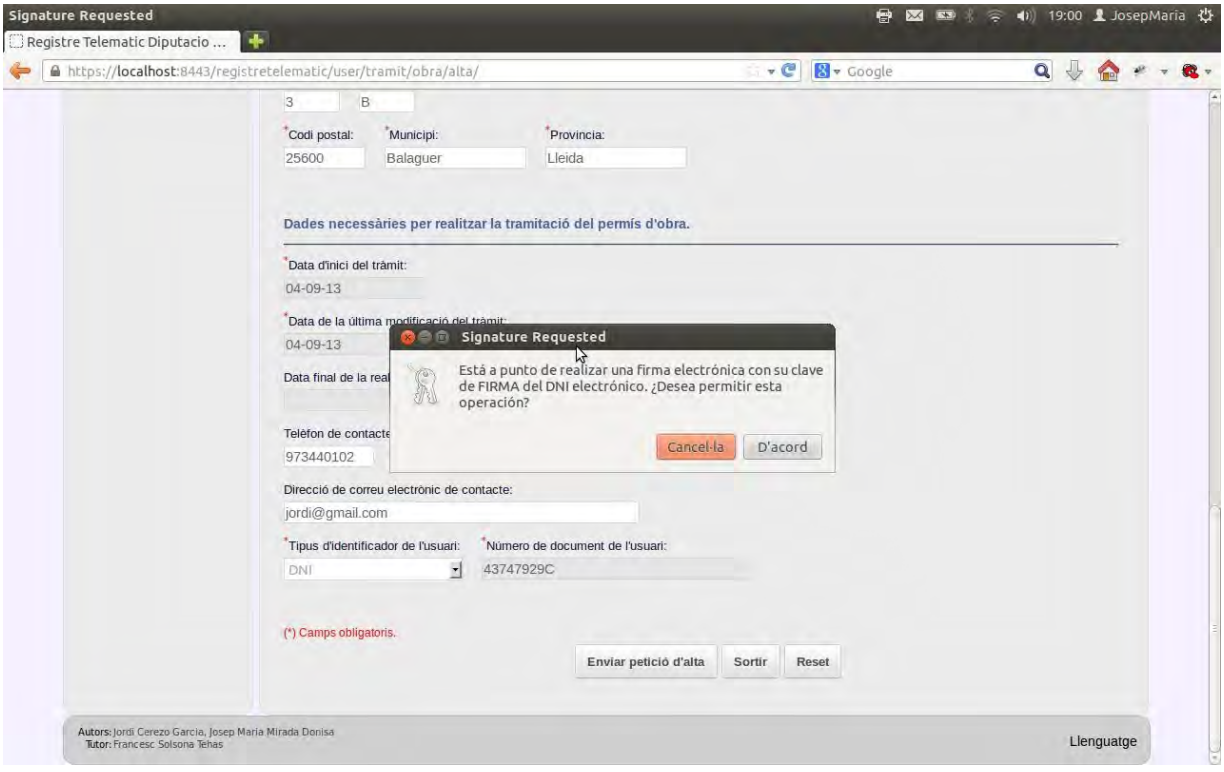
Il·lustració 124: Signatura electrònica. Certificat vàlid.

Finalment, l'aplicació demanarà per darrera vegada permís d'execució (Il·lustració 125).



Il·lustració 125: Signatura electrònica. Darrera petició de confirmació.

Un cop confirmat, es dura a terme el procés de signatura (Il·lustració 126), que omplirà el camp de la base de dades habilitat a aquest efecte. L'aplicació seguirà el seu procés habitual, validant les dades introduïdes al formulari, i, en cas de ser correctes, passant directament a la introducció de documents referents al tràmit creat.



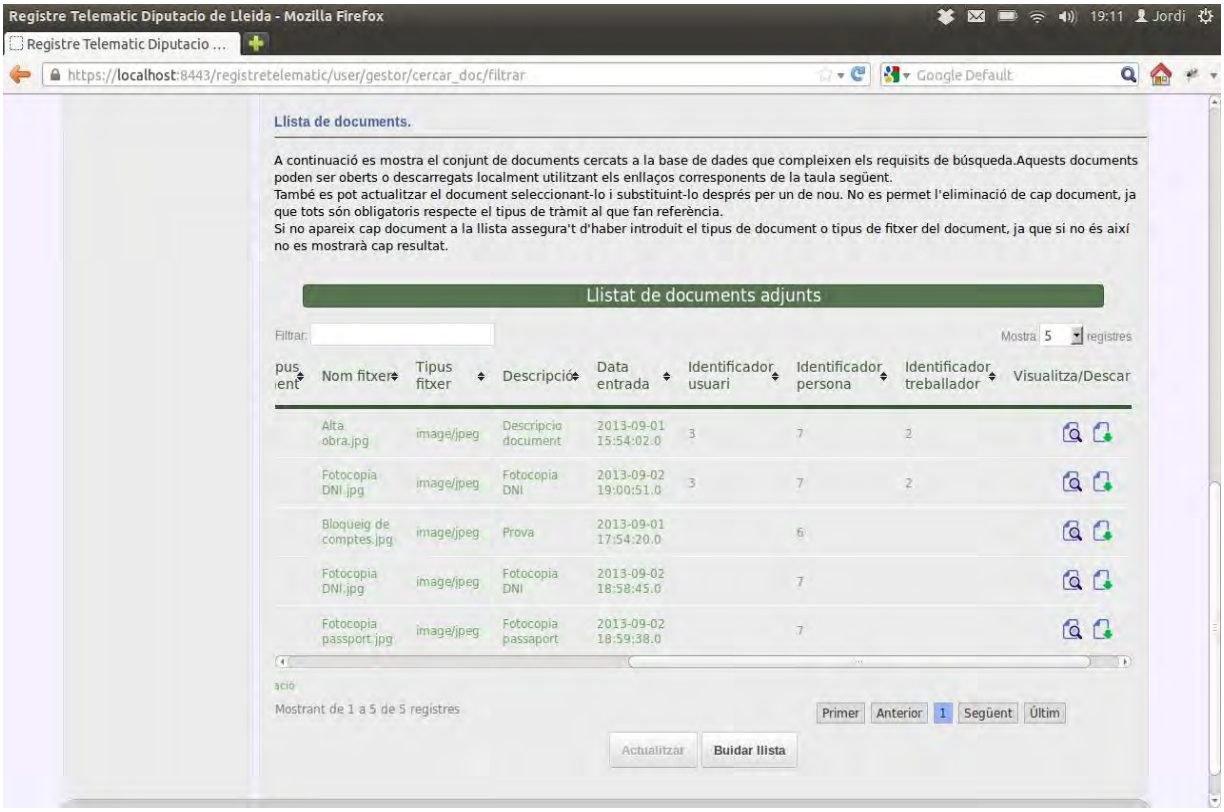
Il·lustració 126: Signatura electrònica. Procés realitzat correctament.

Si un empleat de l'Administració pública necessita realitzar algun canvi a les dades d'un tràmit, la signatura original deixarà de ser vàlida, ja que les dades signades no seran, a partir de llavors, les que va escriure originalment el ciutadà. Per aquest motiu, pot ser necessari que les dades del tràmit siguin signades de nou. El procés es podrà realitzar des de la pantalla d'inici de l'aplicació, mitjançant la taula que contindrà aquests registres modificats i pendents de signatura (5.3.1 Pantalla inicial).

5.3.5 Gestor documental

El **gestor documental** (Il·lustració 127) és la part de l'aplicació encarregada de la gestió de documents acreditatius de la identitat dels ciutadans emmagatzemats la base de dades, així com de qualsevol document que faci referència a algun dels tràmits que gestiona l'aplicació web. Els documents no són necessaris en cap cas per a la creació o gestió dels tràmits o persones, però moltes vegades és important tenir documents que serveixin per contrastar determinades dades. Per exemple, en el cas d'introduir a l'aplicació un perfil d'una persona, o un tràmit de tipus padró, pot ser interessant emmagatzemar una copia del DNI. En el cas de demanar un permís d'obra, pot ser convenient emmagatzemar una còpia de l'expedient d'obra, i en el d'una sanció de la guàrdia urbana, podria ser convenient guardar la imatge escanejada de la còpia de l'agent.

Aquest gestor documental té la capacitat d'emmagatzemar documents de tota mena. La base de dades es limitarà a guardar-los, donant la possibilitat de la seva posterior visualització o descàrrega. Per poder obrir el document cal disposar a l'ordinador d'un programa amb la capacitat per obrir el document seleccionat. Per exemple, si el document és de tipus JPG, serà necessari disposar d'un visualitzador d'imatges capaç d'obrir documents d'aquest tipus. Si el document és un text en format ODT, serà necessari disposar d'un processador de text amb capacitat d'obrir documents de text d'aquest format.



Il·lustració 127: Exemple del resultats d'una cerca global del gestor documental

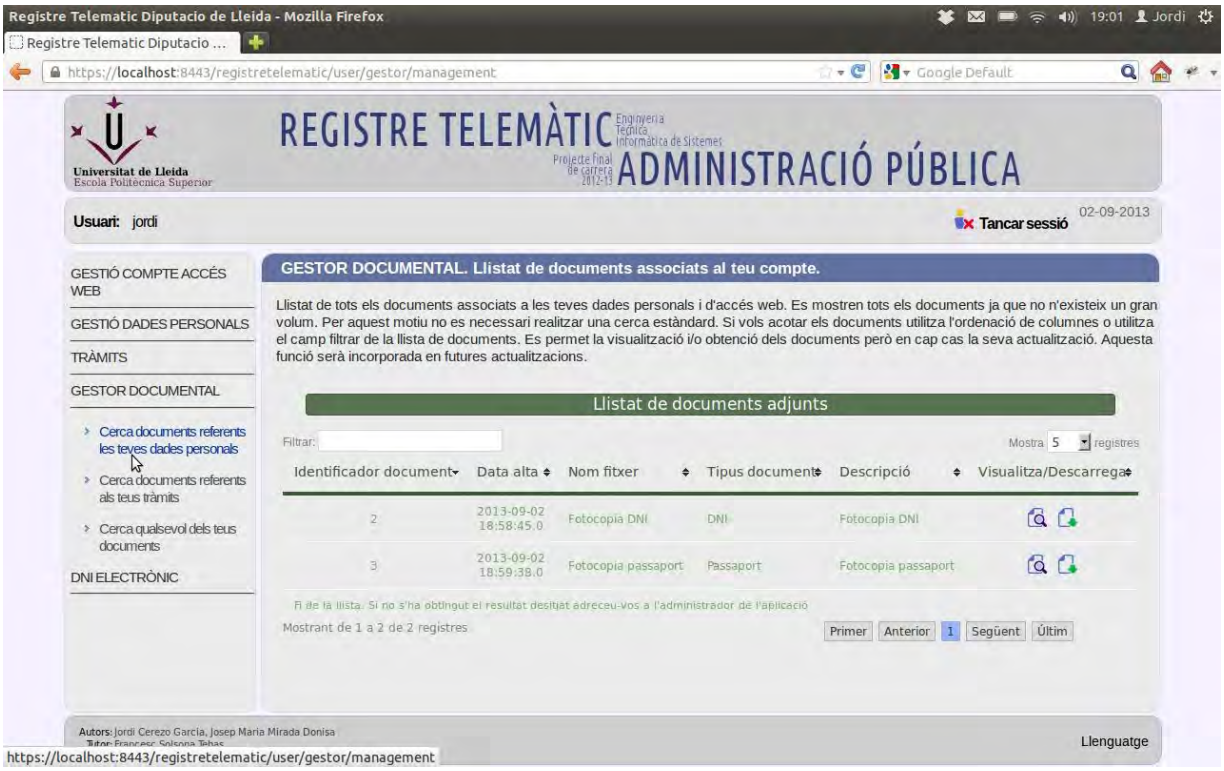
Cal remarcar que, aquest gestor documental té la capacitat d'emmagatzemar documents **relacionats amb les persones,** o bé documents **relacionats amb els tràmits**. Els dos tipus seran accessibles des de l'entrada de menú etiquetada com a **"Gestor Documental"**, i podran ser cercats conjuntament, o bé delimitant-los segons el tipus de registre amb el que tenen relació, això és, persones o tràmits.

Segons l'entrada de menú que seleccioni el ciutadà, es mostrarà una pantalla amb una taula de resultats, mostrant els documents que fan referència a persones, a tràmits, o bé ambdós tipus conjuntament. La funcionalitat més important d'aquesta taula de resultats la trobem a la darrera columna dels registres mostrats. Aquí trobem dues icones, les quals permetran al ciutadà realitzar la gestió dels documents. La icona de l'esquerra, amb una petita lupa, permetrà visualitzar el document seleccionat utilitzant el programa amb capacitat per la lectura del format de document triat. La icona de la dreta, marcada amb una petita fletxa verda apuntant cap a baix, permetrà l'empleat descarregar una còpia del fitxer seleccionat, i guardar-lo a la carpeta de l'ordinador que trii. El ciutadà no té la capacitat d'eliminar el document de la base de dades. En cas de voler realitzar aquesta acció, haurà de posar-se en contacte amb l'Administració, i demanar l'eliminació del document desitjat.

Passem a veure cadascuna de les entrades del gestor documental amb més detall.

5.3.5.1 Cerca documents referents a les teves dades personals

Aquesta entrada del menú portarà al ciutadà a una pàgina on es mostra una taula de resultats que conté tots aquells documents associats al seu perfil d'usuari a l'aplicació (Il·lustració 128). S'ha de tenir present que no es mostraran els documents associats a tràmits del ciutadà. Aquesta taula de resultats permet la navegació a través dels registres, mitjançant els botons inferiors, i, com s'ha comentat a la introducció del "Gestor documental", dona la possibilitat de visualitzar o descarregar els documents. Si no existeixen documents relacionats amb el ciutadà que ha iniciat sessió a l'aplicació, la taula de resultats apareixerà buida.



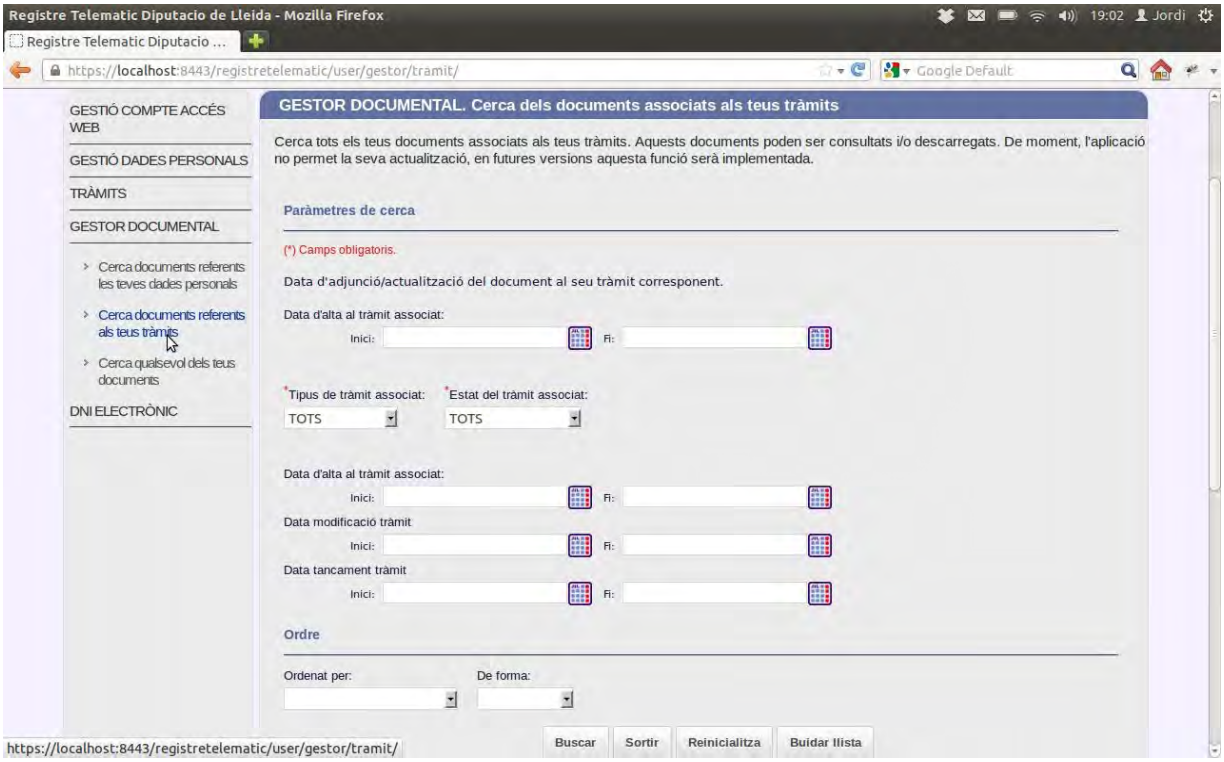
Il·lustració 128: Gestor documental. Documents relacionats amb el perfil d'usuari del ciutadà

5.3.5.2 Cerca documents associats als teus tràmits

Com la seva etiqueta indica, aquesta entrada del menú portarà al ciutadà a una pàgina on es mostra una taula de resultats que conté tots aquells documents associats als tràmits del ciutadà connectat a l'aplicació. S'ha de tenir present que no es mostraran els documents associats al perfil d'usuari del ciutadà.

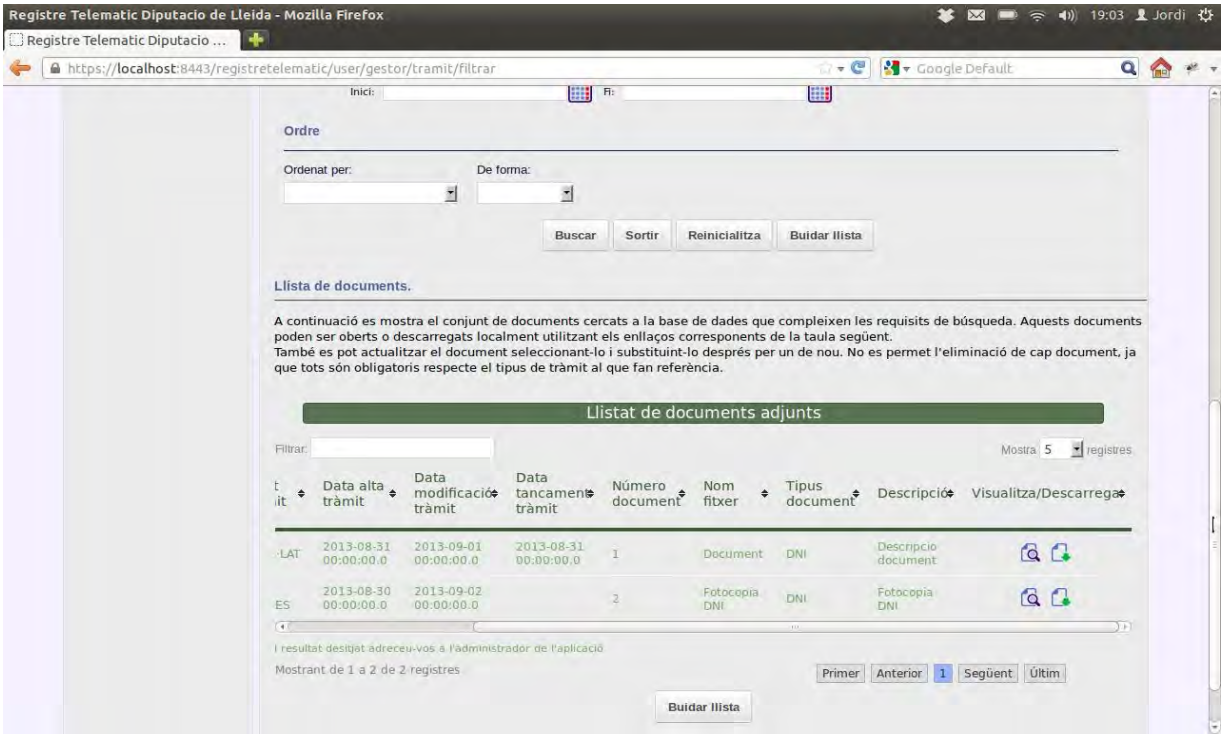
La part superior de la pàgina (Il·lustració 129) conté una sèrie de camps que permetran acotar la cerca de documents associats amb els tràmits del ciutadà que ha iniciat sessió a l'aplicació web:

- **Data d'inserció del document**: aquests camps fan referència a les dates en que el document va ser inserit a la base de dades. S'ha de tenir present que aquesta data no ha de ser, necessàriament, la mateixa que la data d'alta del tràmit a l'aplicació, ja que el document pot haver estat inserit amb posterioritat. La cerca retornarà els documents compresos entre les dates d'inici i fi que s'omplin al cercador. Si només s'omple la data d'inici, es cercaran els documents inserits després de la data introduïda, i fins a l'actualitat. Si, en canvi, s'omple només la data de fi, es cercaran només aquells documents inserits abans de la data introduïda. Si els camps es deixen en blanc, no es tindran aquestes dates en compte a l'hora de realitzar la cerca. Per tant, no es filtraran els documents segons la seva antiguitat a la base de dades.
- **Tipus de tràmit associat**: aquest camp fa referència al tipus de tràmit al que està associat el document. D'aquesta manera, pot cercar els documents, delimitant-los a documents associats al padró, a una llicència d'activitat amb risc mediambiental, o bé amb la seva adreça fiscal.
- **Estat del tràmit associat:** el ciutadà podrà filtrar els documents, segons si el tràmit associat està activat, desactivat, anul·lat, pendent de firmar... Això pot ser molt útil , donat que principalment el ciutadà consultarà, majoritàriament, documents associats a tràmits que tingui oberts o pendents de signatura.
- **Dates**: aquests camps fan referència a les dates d'alta, darrera modificació i tancament respectivament, dels diferents tràmits als quals estan associats els documents del gestor documental. La cerca retornarà els documents associats a tràmits compresos entre les dates d'inici i fi que s'omplin al cercador. Si només s'omple la data d'inici, es cercaran els documents associats a tràmits amb data posterior a la data introduïda, i fins a l'actualitat. Si, en canvi, s'omple només la data de fi, es cercaran només aquells documents associats a tràmits amb data anterior a la introduïda. Si els camps es deixen en blanc, no es tindran aquestes dates en compte a l'hora de realitzar la cerca. Per tant, no es filtraran els documents segons l'antiguitat del tràmit associat.



Il·lustració 129: Gestor documental. Documents relacionats amb els tràmits del ciutadà. Detall dels camps de cerca.

Aquesta taula de resultats permet la navegació a través dels registres (Il·lustració 130), mitjançant els botons inferiors, i, com s'ha comentat a la introducció del "Gestor documental", dona la possibilitat de visualitzar o descarregar els documents. Si no existeixen documents associats a tràmits per al ciutadà que ha iniciat sessió a l'aplicació, la taula de resultats apareixerà buida.



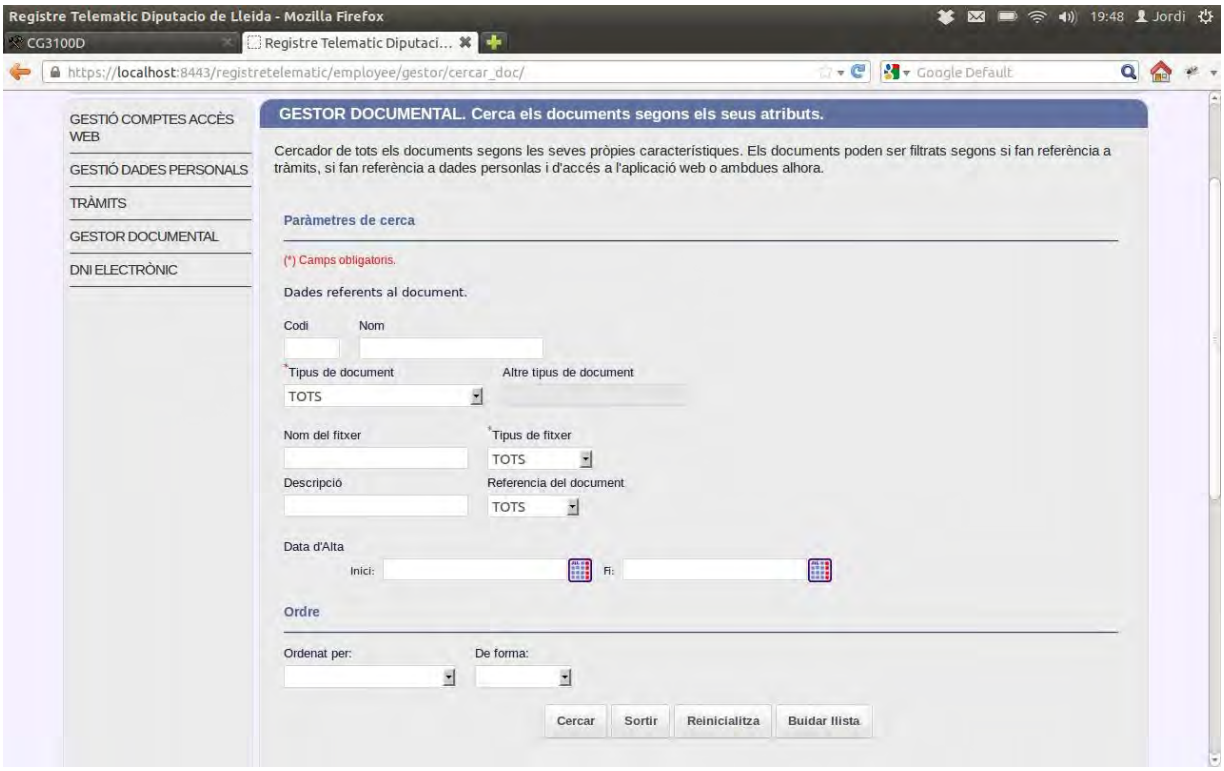
Il·lustració 130: Gestor documental. Llistat de documents associats als tràmits d'un ciutadà.

5.3.5.3 Cerca qualsevol dels teus documents

La darrera entrada del menú del **"Gestor documental"** permet al ciutadà realitzar una cerca entre els seus documents, independentment de si estan associats al seu perfil d'usuari, o als seus tràmits. En prémer aquest botó, s'obrirà una nova pantalla, i, com en el cas anterior, la part superior del formulari contindrà una sèrie de paràmetres mitjançant els quals es podrà acotar el llistat de resultats:

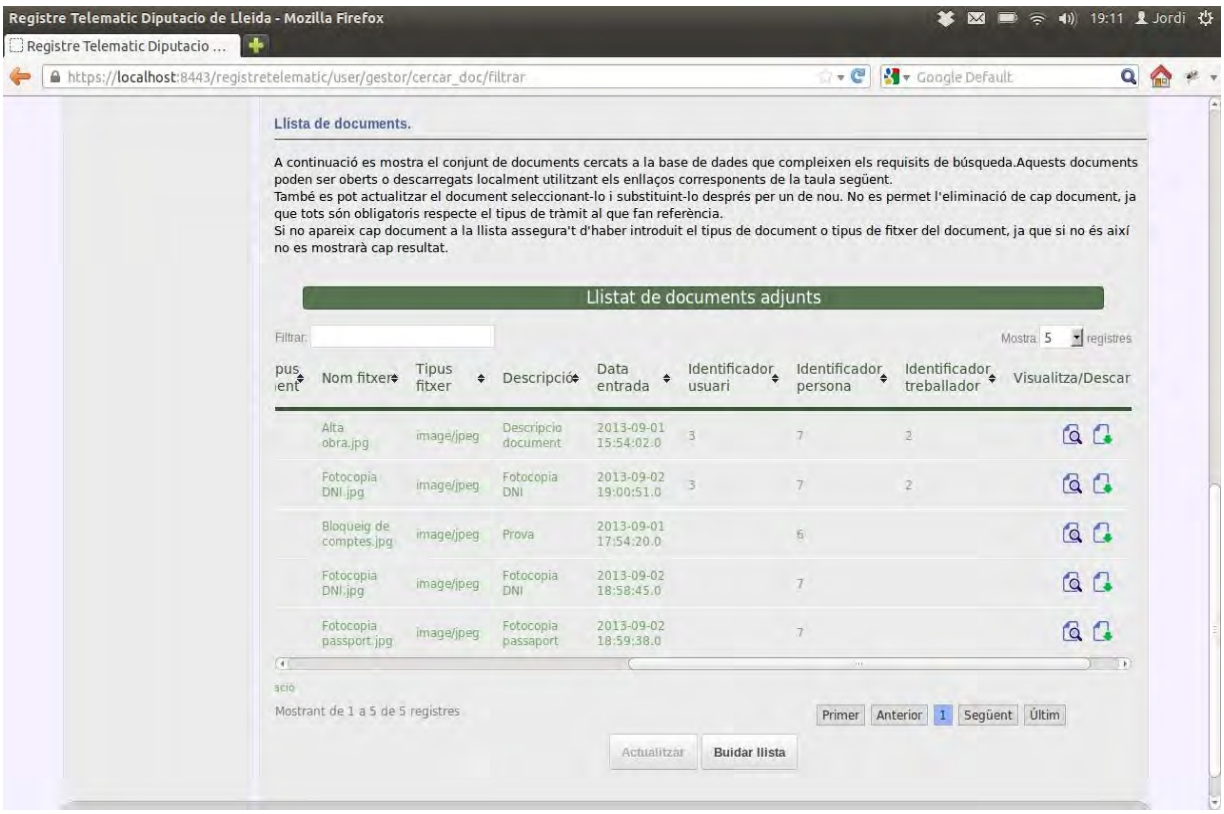
- **Codi**: fa referència al codi associat al document a la base de dades. Si el ciutadà coneix el codi del document, generat de manera automàtica durant la seva inserció a la base de dades i mostrat al formulari d'inserir documents adjunts, aquesta és la forma més ràpida de cercar-lo.
- **Nom**: fa referència al nom del document que se li va assignar al introduir-lo a la base de dades.
- **Tipus de document**: fa referència al tipus de document acreditatiu de la identitat dels usuaris a la base de dades de l'aplicació. L'empleat pot cercar, per exemple, només documents de tipus DNI, passaport o llibre de família entre altres. Si al desplegable se selecciona l'entrada "ALTRES", s'habilitarà el camp **"Altre tipus de document"**, per tal d'introduir manualment el tipus de document desitjat.
- **Nom del fitxer**: fa referència al nom real del fitxer, el que tenia al sistema de fitxers del sistema operatiu en el moment de guardar-lo al gestor documental. S'ha de diferenciar del "nom", que es refereix al nom que l'empleat va introduir a la base de dades per tal d'emmagatzemar-lo.
- **Tipus del fitxer**: fa referència al tipus de fitxer que s'està cercant, per exemple, imatges o documents pdf entre altres.
- **Descripció**: fa referència a la descripció que l'empleat va introduir al guardar el document a la base de dades.
- **Referència del document**: aquest camp permet diferència entre els documents que estan associats a un usuari de l'aplicació, o bé a un tràmit.
- **Data d'inserció del document**: aquests camps fan referència a les dates en que el document va ser inserit a la base de dades. S'ha de tenir present que aquesta data no ha de ser, necessàriament, la mateixa que la data d'alta del tràmit a l'aplicació, ja que el document pot haver estat inserit amb posterioritat. La cerca retornarà els documents compresos entre les dates d'inici i fi que s'omplin al cercador. Si només s'omple la data d'inici, es cercaran els documents inserits després de la data introduïda, i fins a l'actualitat. Si, en canvi, s'omple només la data de fi, es cercaran només aquells documents inserits abans de la data introduïda. Si els camps es deixen en blanc, no es tindran aquestes dates en compte a l'hora de realitzar la cerca. Per tant, no es filtraran els documents segons la seva antiguitat a la base de dades.
- **Criteris d'ordenació. Ordenat per i De forma:** els criteris d'ordenació fan referència a la forma en que es vol que ens aparegui ordenada la llista de tràmits que ens retornarà la cerca a la base de dades. "Ordenat per" es refereix al camp pel qual volem ordenar. És a dir, si es tria el nom d'usuari, la taula de resultats ens apareixerà ordenada alfabèticament segons el nom d'usuari. Si es tria una data, estarà ordenada segons l'antiguitat d'aquella data. El criteri "De forma" fa referència al mètode d'ordenament. Si es tria ascendent, una cerca alfabètica serà mostrada des de la "A" fins a la "Z". Una cerca per data serà mostrada dels registres

més antics al més nous. Si, en canvi, es marca l'opció descendent, l'ordenació alfabètica serà inversa, i la cerca per antiguitat anirà del tràmit més nou al més antic dels que formen part de la llista de tràmits cercats. Si es deixen en blancs aquests camps, la taula mostrarà el llistat de tràmits segons l'ordre en que han estat introduïts a la base de dades.



Il·lustració 131: Gestor documental. Cercador de tots els tipus de document. Detall dels camps de cerca

A la part inferior es mostra la taula de resultats, que permet la navegació a través dels registres (Il·lustració 132), mitjançant els botons inferiors. Com s'ha comentat a la introducció del "Gestor documental", dona la possibilitat de visualitzar o descarregar els documents. Si no existeixen documents associats ni al perfil d'usuari del ciutadà connectat a l'aplicació, ni tampoc associats als seus tràmits, la taula de resultats apareixerà buida.



Il·lustració 132: Gestor documental. Llistat de documents associats al perfil d'usuari del ciutadà i als seus tràmits.

5.3.6 DNI Electrònic

Aquesta darrera entrada de menú **permetrà la comprovació dels certificats d'autenticació i de signatura del DNI-electrònic**. D'aquesta manera, en cas que no es pugui dur a terme alguna de les tasques associades al DNI-e, l'usuari podrà determinar si existeix alguna mena d'error en els certificats emmagatzemats al xip del DNI. Tant per al certificat d'autenticació com per al de signatura, el ciutadà podrà realitzar tres accions diferents:

- **Visualitzar les dades**: mostrarà les dades contingudes al certificat.
- **Comprovar l'estat**: mostrarà l'estat del certificat, de tal manera que el ciutadà podrà conèixer si ha estat revocat, o si és vigent en el moment en que es realitza la comprovació.
- **Comprovar la data d'expiració**: mostrarà la data en que el certificat deixarà de ser vàlid. D'aquesta manera, el ciutadà podrà conèixer del moment en que expirarà, i aquest podrà renovar-lo abans que la revocació sigui executada.

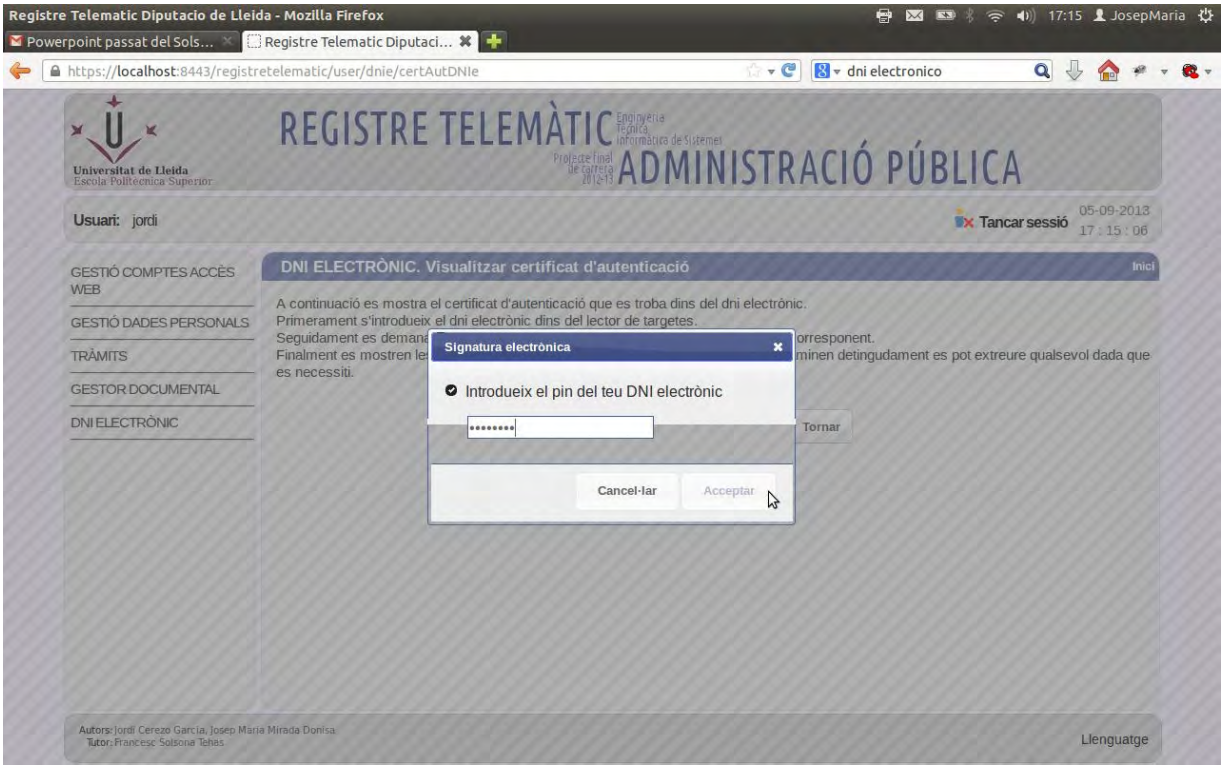
Passem a veure-les en profunditat.

5.3.6.1 Visualitza les dades

En prémer el botó del menú etiquetat com a “Visualitzar dades”, l'aplicació ens dirigirà a la pantalla següent (Il·lustració 133):

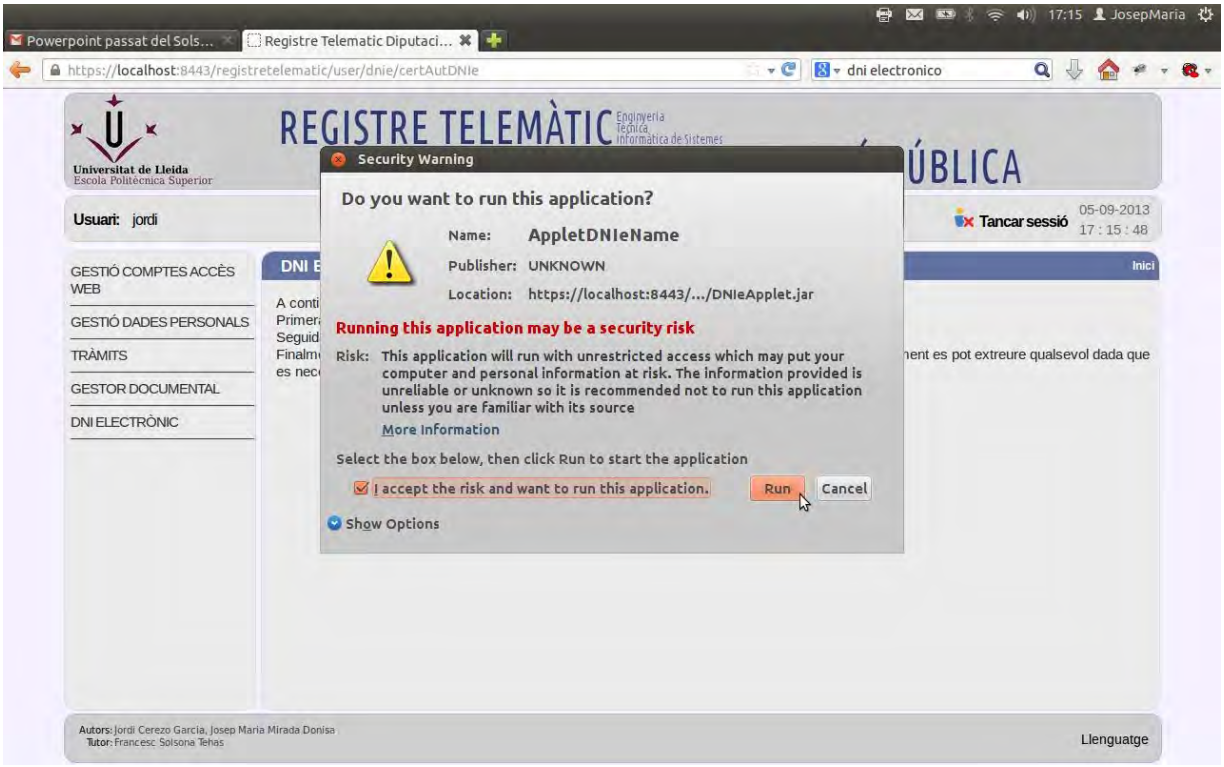
Il·lustració 133: Visualitzar dades certificats. Pantalla inicial.

El ciutadà ha de prémer el botó **"Visualitza certificat"**, i seguidament l'aplicació demanarà el PIN del DNIe inserit (Il·lustració 134).



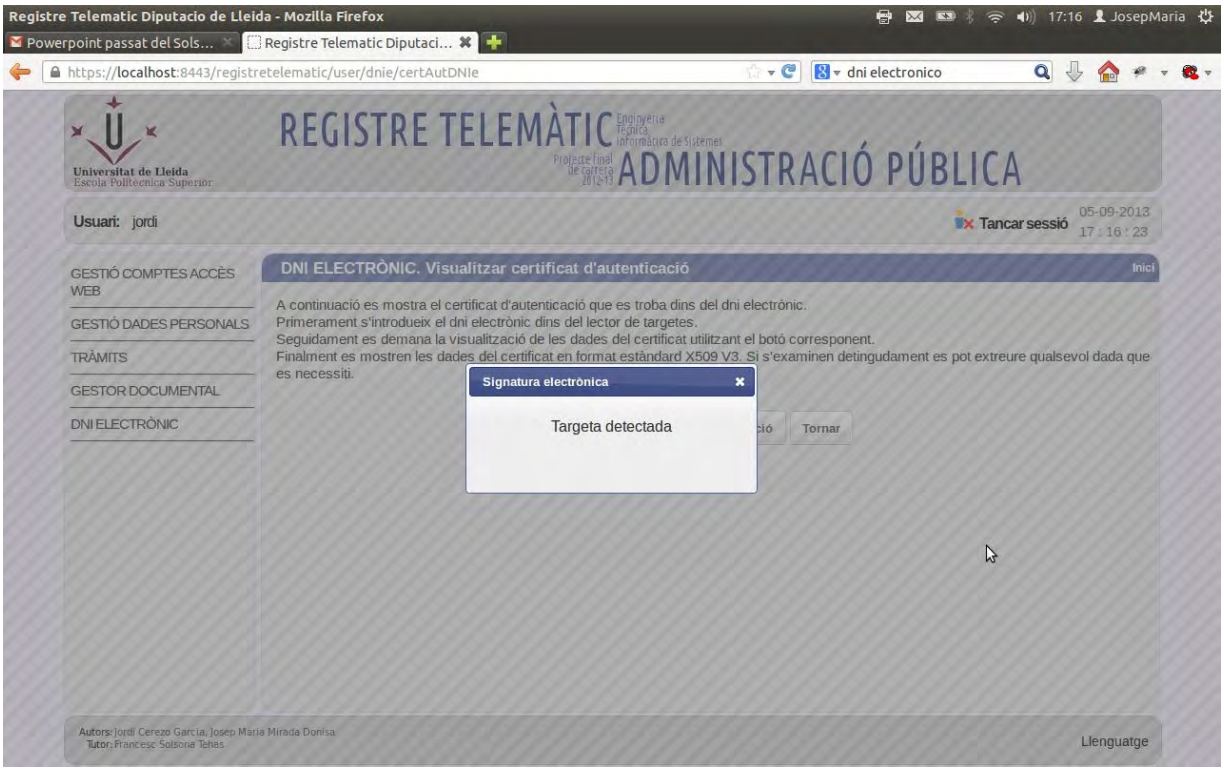
Il·lustració 134: Visualitzar dades certificats. Petició de PIN.

Si el PIN introduït és correcte, l'aplicació ens demanarà permís per a l'execució de l'applet del DNIe (Il·lustració 135):



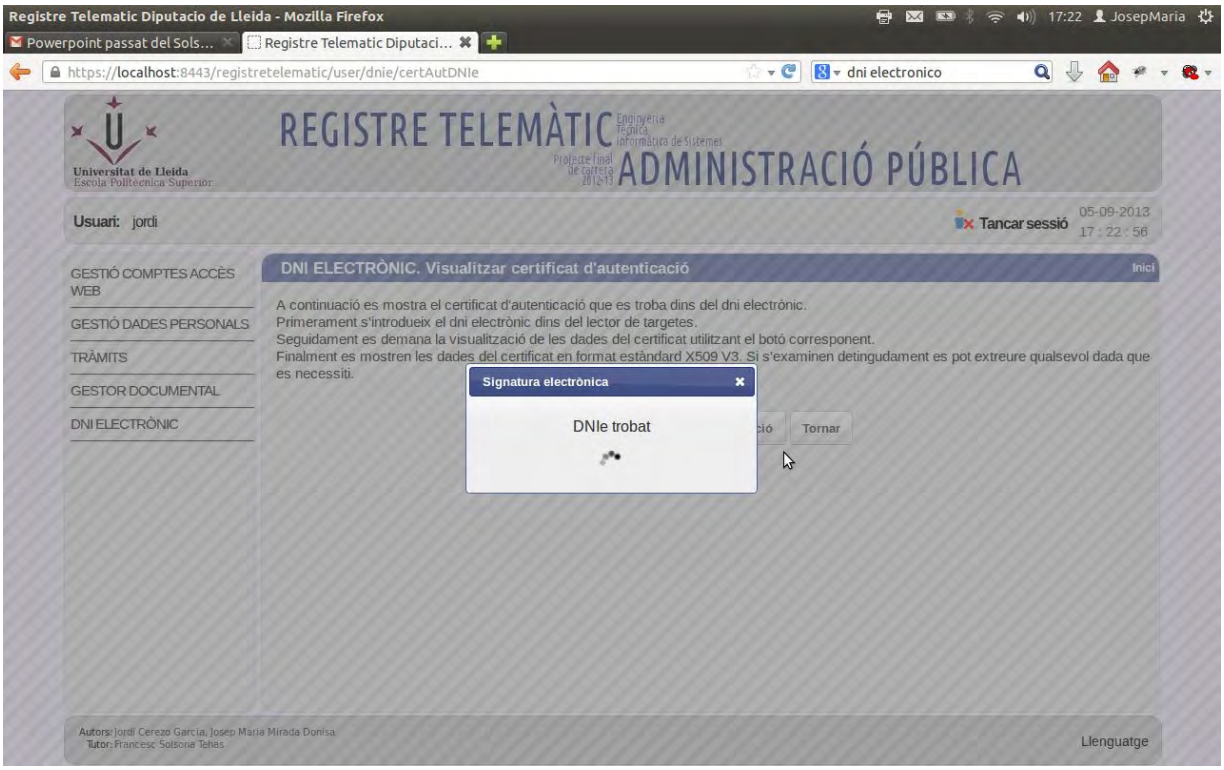
Il·lustració 135: Visualitzar dades certificats. Petició permís execució applet.

El següent pas serà detectar si hi ha una targeta inserida al lector d'smart cards (Il·lustració 136).



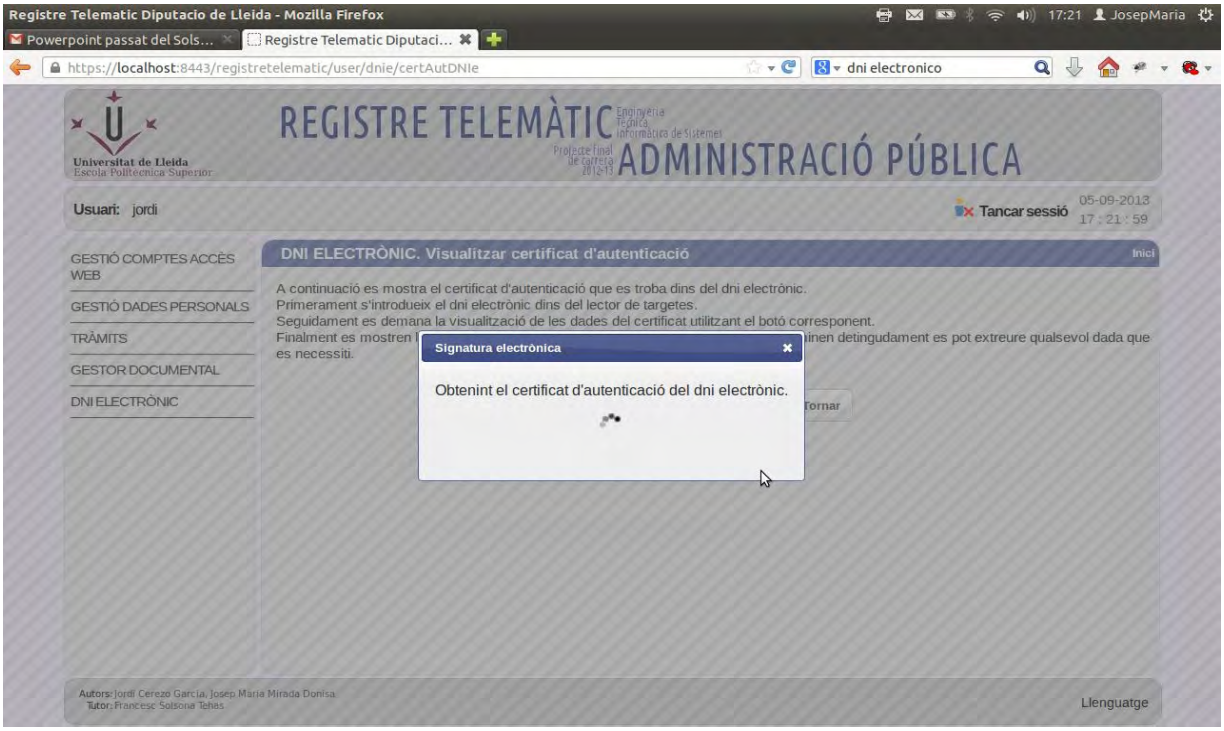
Il·lustració 136: Visualitzar dades certificats. Detecció de targeta.

Si troba una targeta inserida, l'applet detectarà si es tracta d'un DNIe (Il·lustració 137).



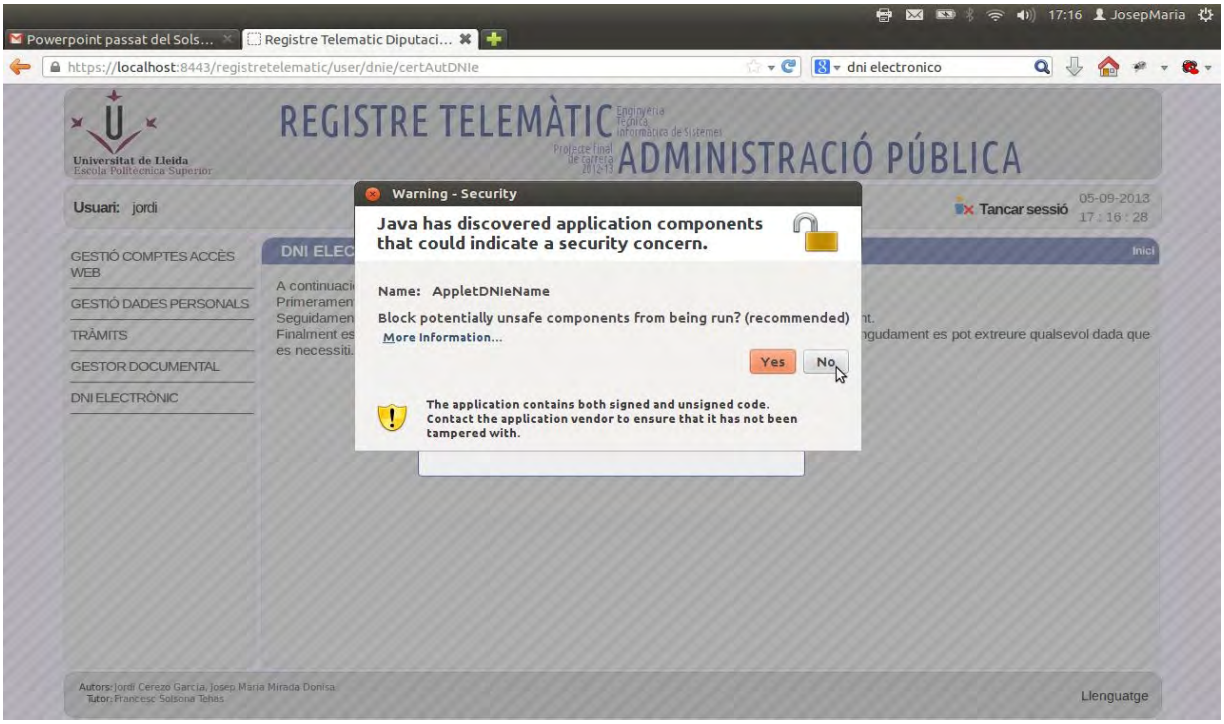
Il·lustració 137: Visualitzar dades certificats. Detecció DNI-e.

Si la targeta inserida és realment un DNI-e, l'applet n'obtindrà el certificat corresponent, el d'autenticació o signatura segons el cas (Il·lustració 138).



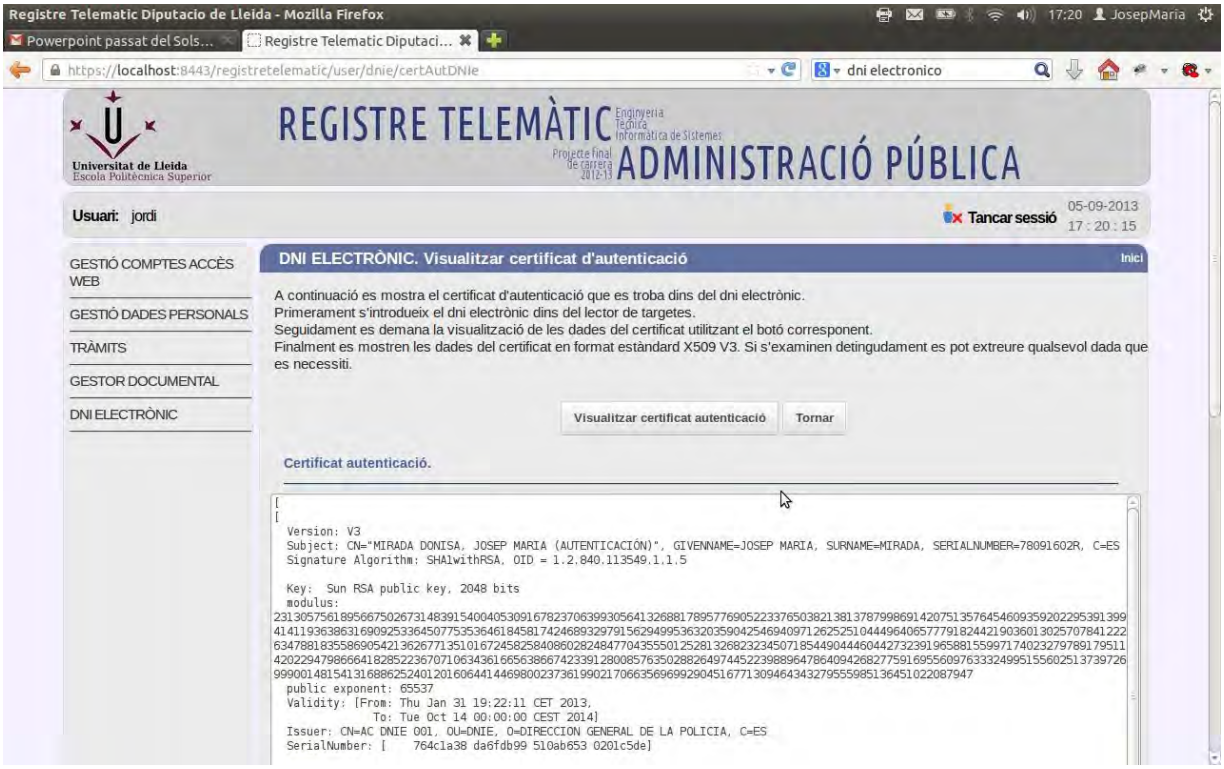
Il·lustració 138: Visualitzar dades certificats. Obtenció del certificat.

Java intentarà, seguidament, bloquejar l'execució de l'applet del DNI-e, donat que el considera potencialment perillós. En aquest cas, el ciutadà haurà de negar aquest bloqueig, ja que confia en l'aplicació que l'Administració Pública posa a la seva disposició (Il·lustració 139).



Il·lustració 139: Visualitzar dades certificats. Bloqueig de seguretat.

Finalment, i si tots els passos s'han realitzat de forma correcta, es mostraran en pantalla les dades del certificat corresponent (Il·lustració 140).

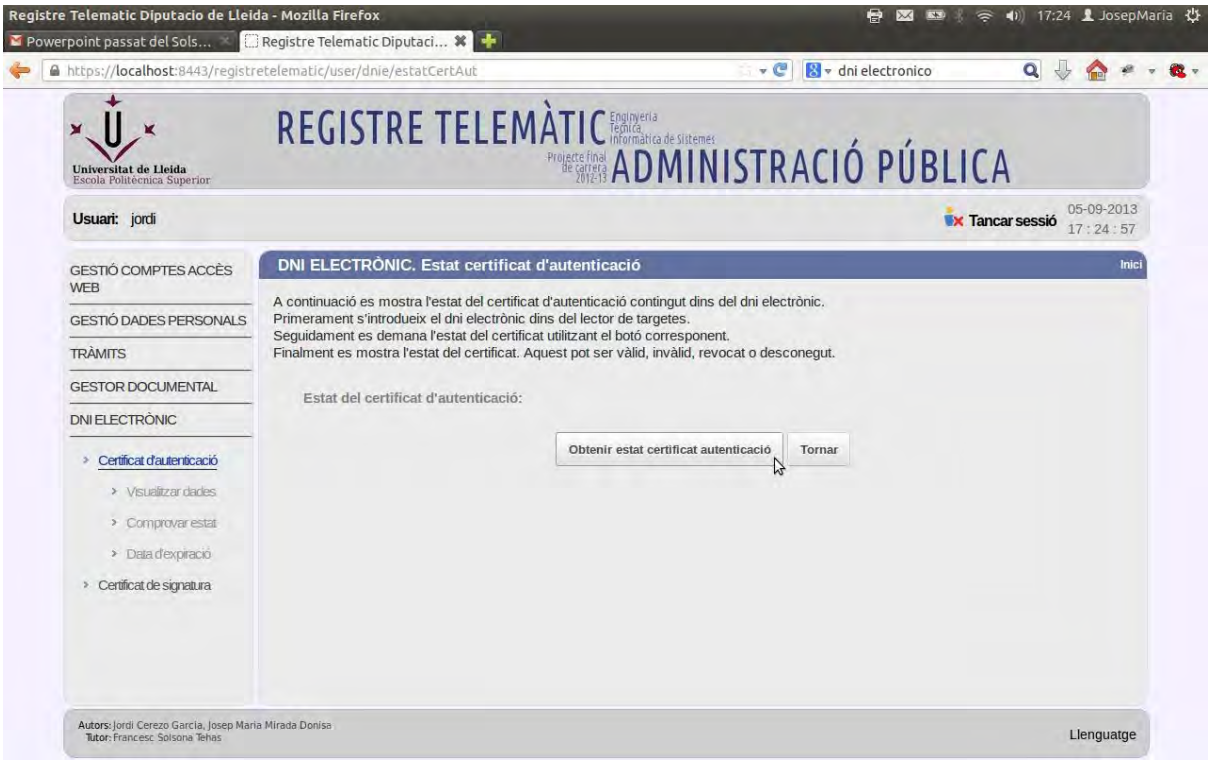


Il·lustració 140: Visualitzar dades certificats. Resultat final.

Si qualsevol dels anteriors passos falla, es mostrarà un missatge en pantalla informant sobre l'error.

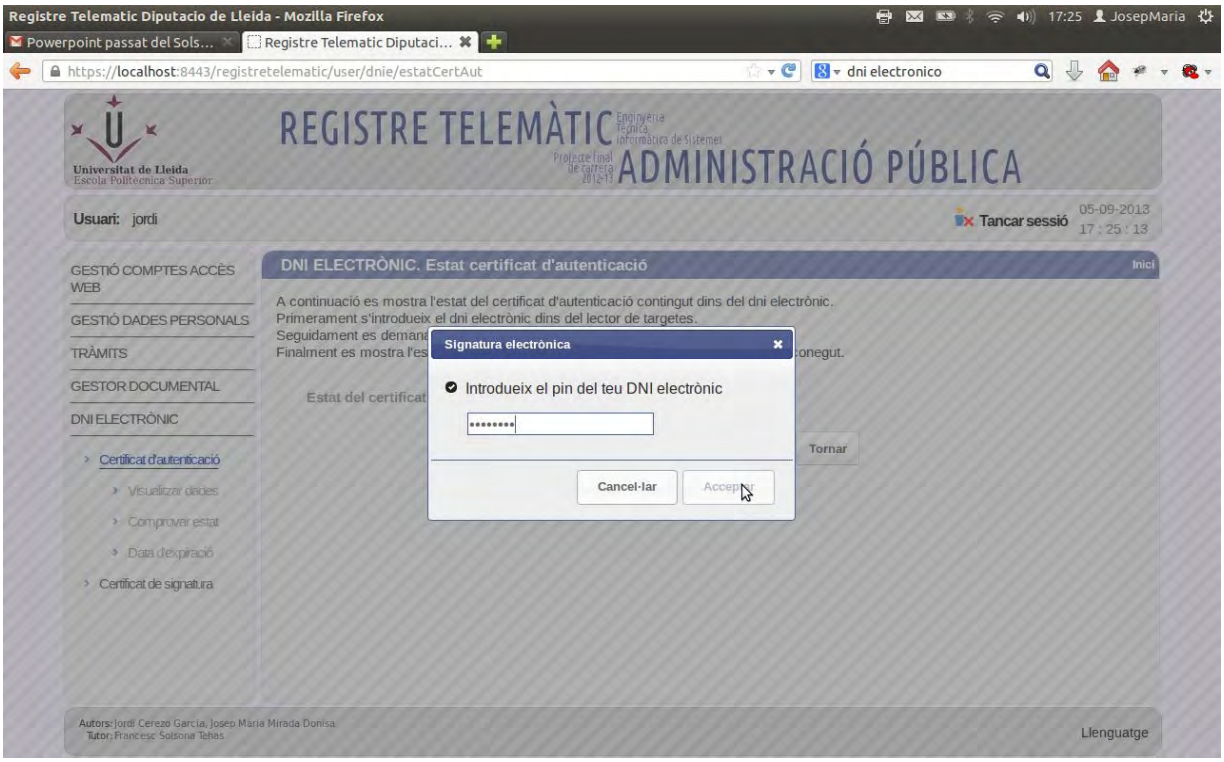
5.3.6.2 Comprovar estat

En prémer el botó del menú etiquetat com a “Comprovar Estat”, l'aplicació ens dirigirà a la pantalla següent (Il·lustració 141):



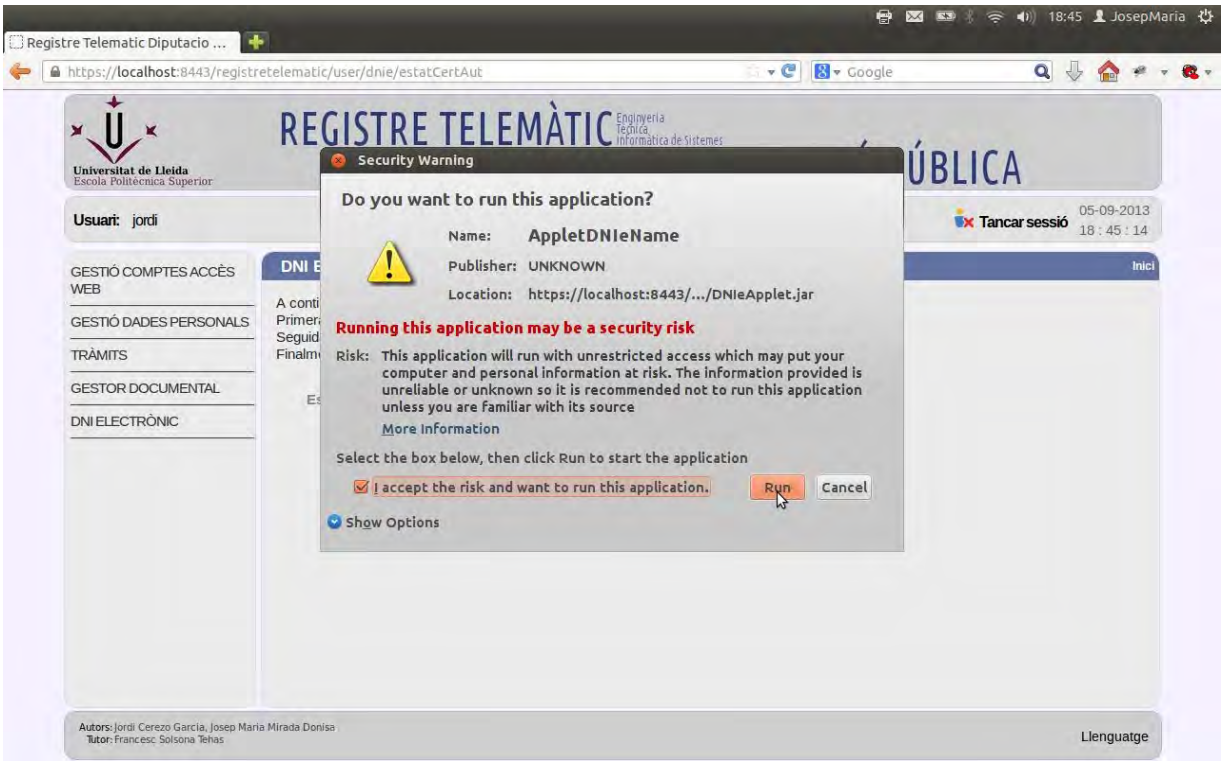
Il·lustració 141: Comprovar estat del certificat. Pantalla inicial.

El ciutadà ha de prémer el botó **"Obtenir estat certificat"**, i seguidament l'aplicació demanarà el PIN del DNIe inserit (Il·lustració 142).



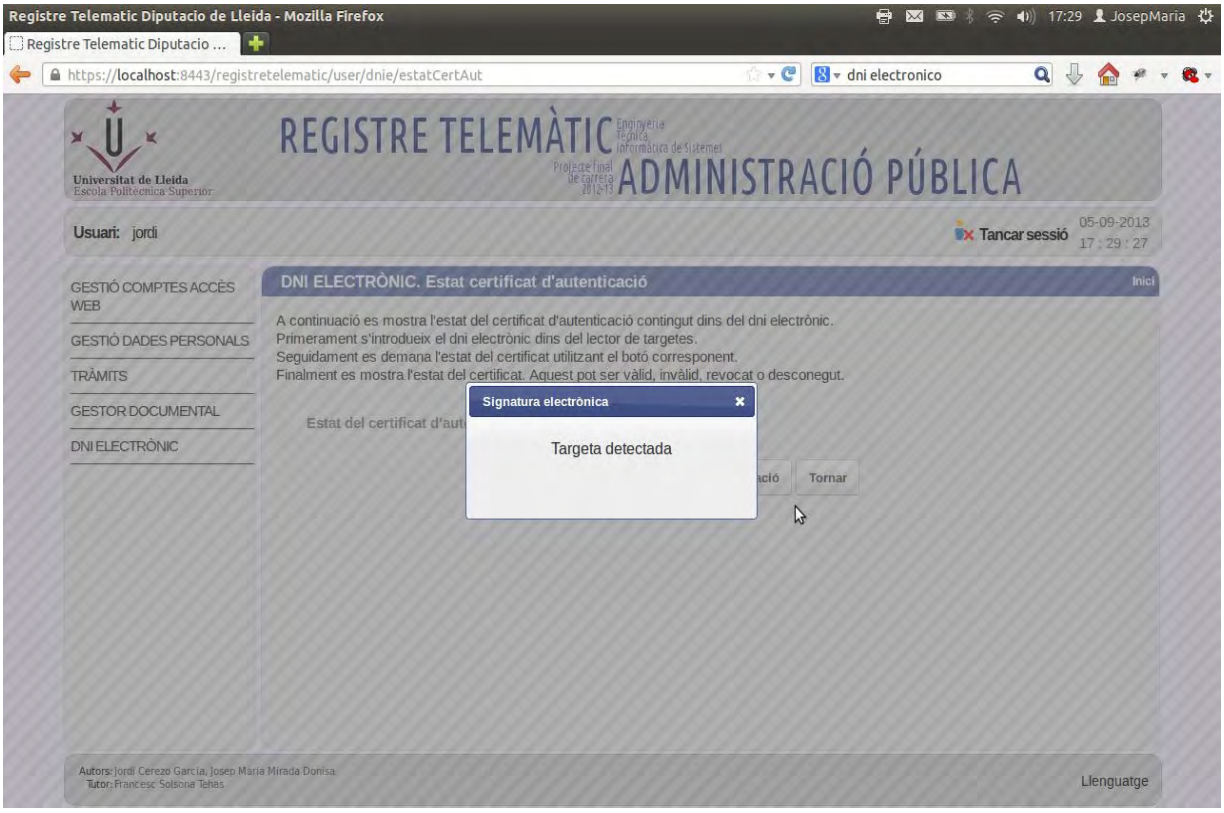
Il·lustració 142: Comprovar estat del certificat. Petició de PIN.

Si el PIN introduït és correcte, l'aplicació ens demanarà permís per a l'execució de l'applet del DNIe (Il·lustració 143):



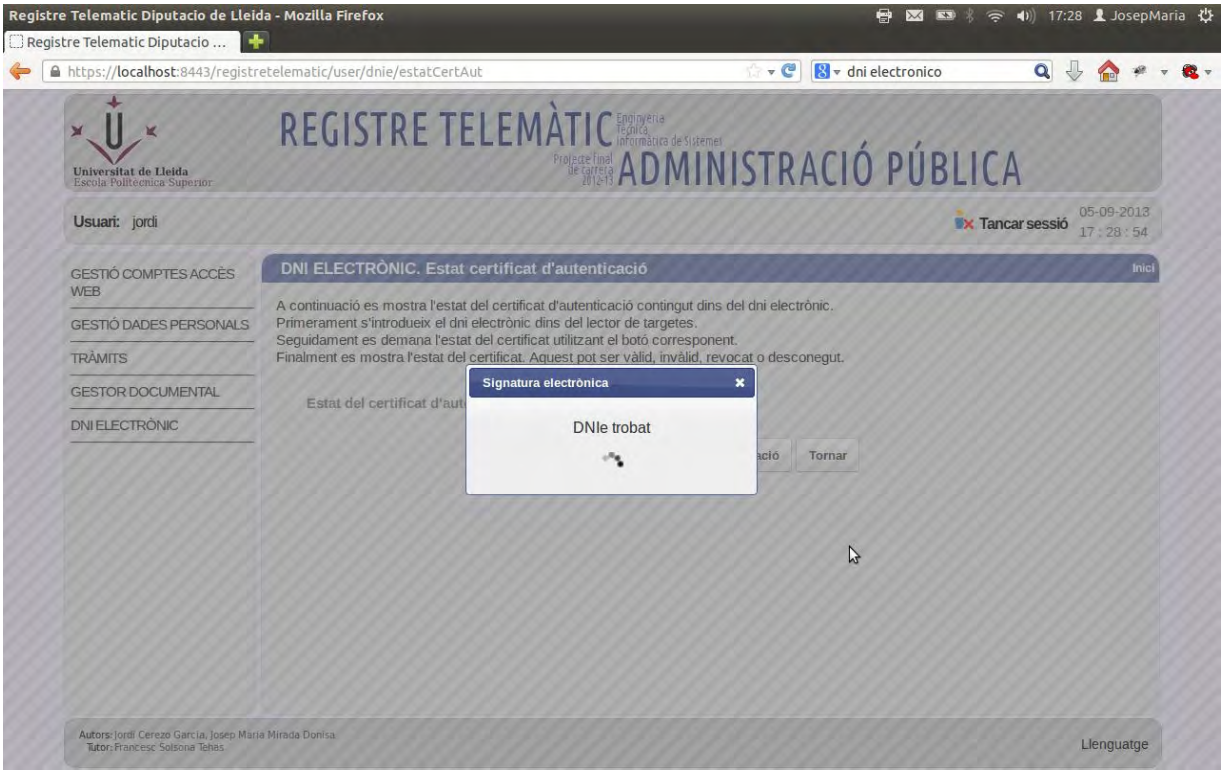
Il·lustració 143: Comprovar estat del certificat. Petició permís execució applet.

El següent pas serà detectar si hi ha una targeta inserida al lector d'smart cards (Il·lustració 144).



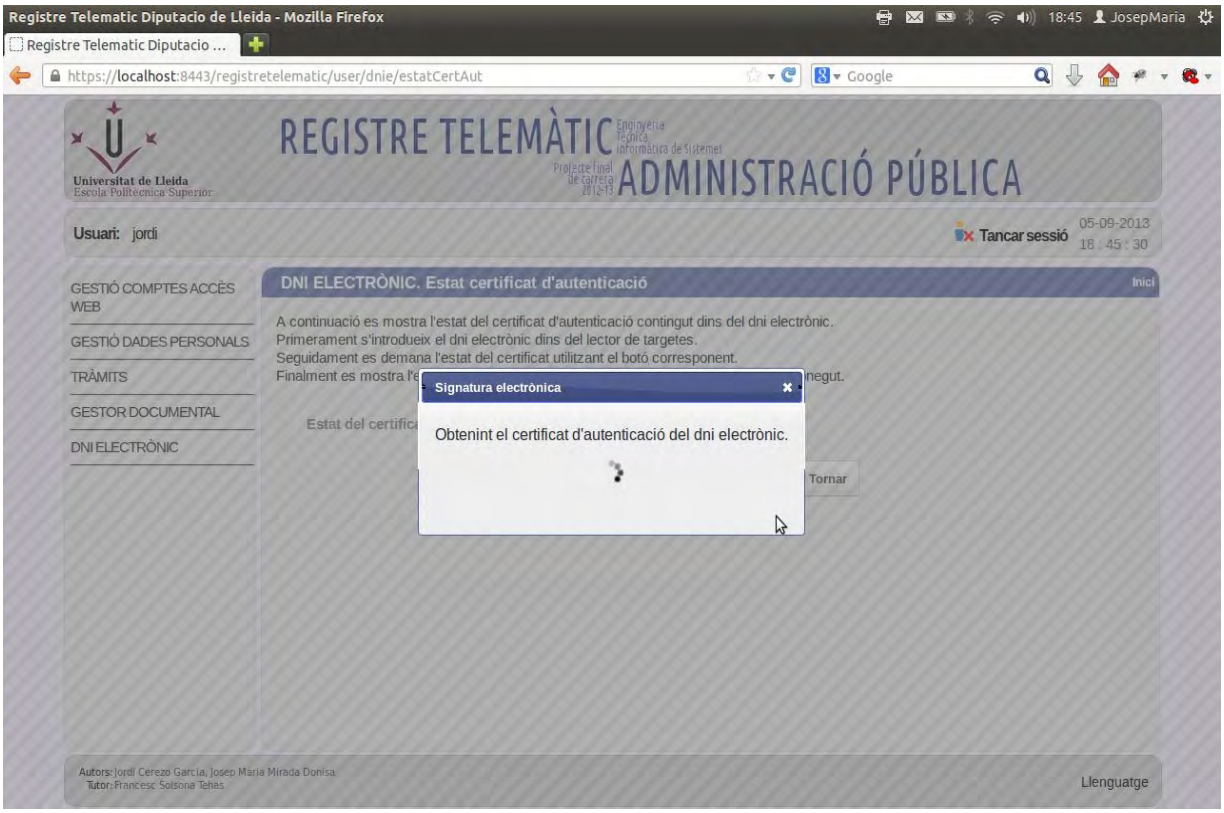
Il·lustració 144: Comprovar estat del certificat. Detecció de targeta.

Si troba una targeta inserida, l'applet detectarà si es tracta d'un DNIe (Il·lustració 145).



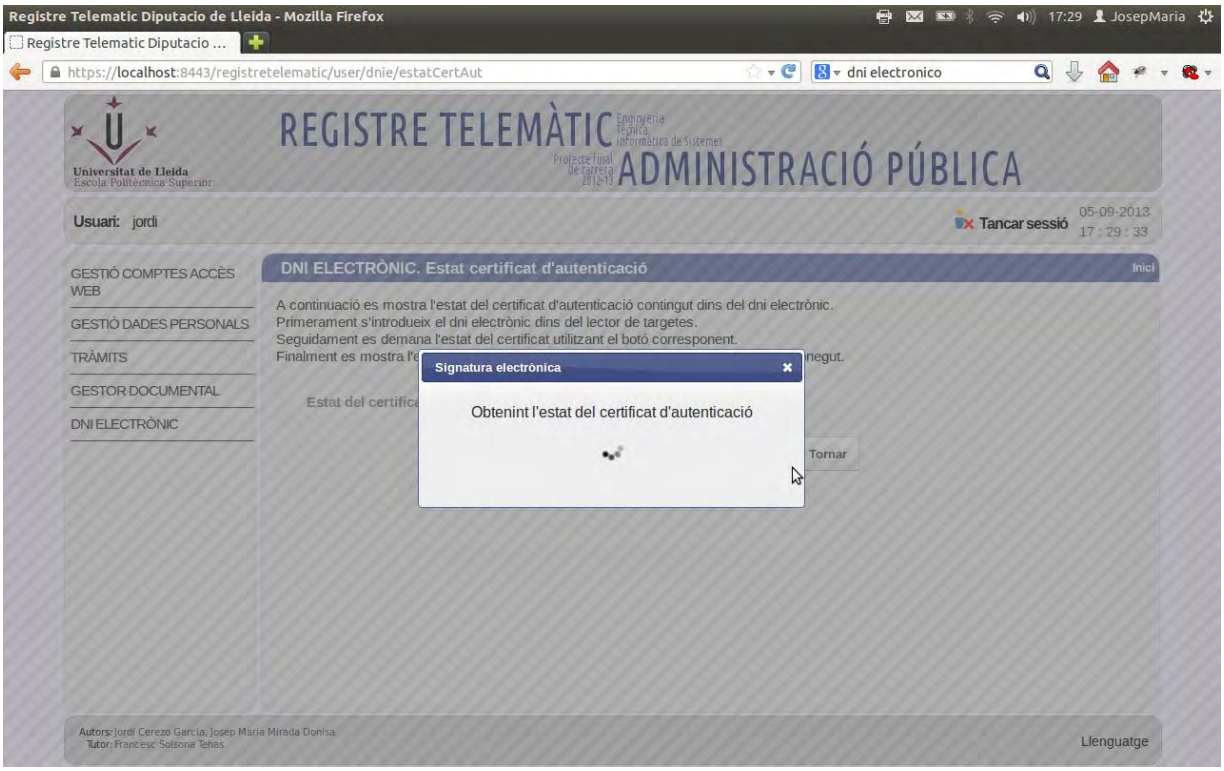
Il·lustració 145: Comprovar estat del certificat. Detecció DNI-e.

Si la targeta inserida és realment un DNI-e, l'applet n'obtindrà el certificat corresponent, el d'autenticació o signatura segons el cas (Il·lustració 146).



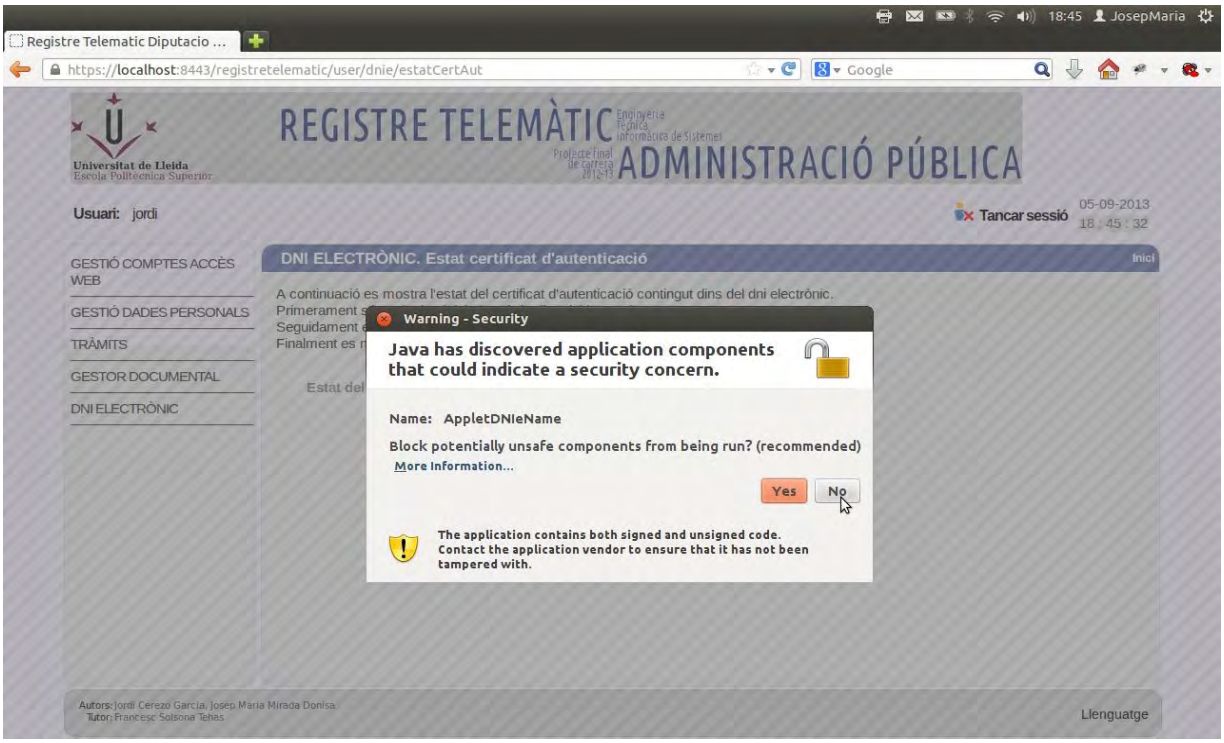
Il·lustració 146: Visualitzar dades certificats. Obtenció del certificat.

El següent pas serà comprovar l'estat del certificat obtingut (Il·lustració 147).



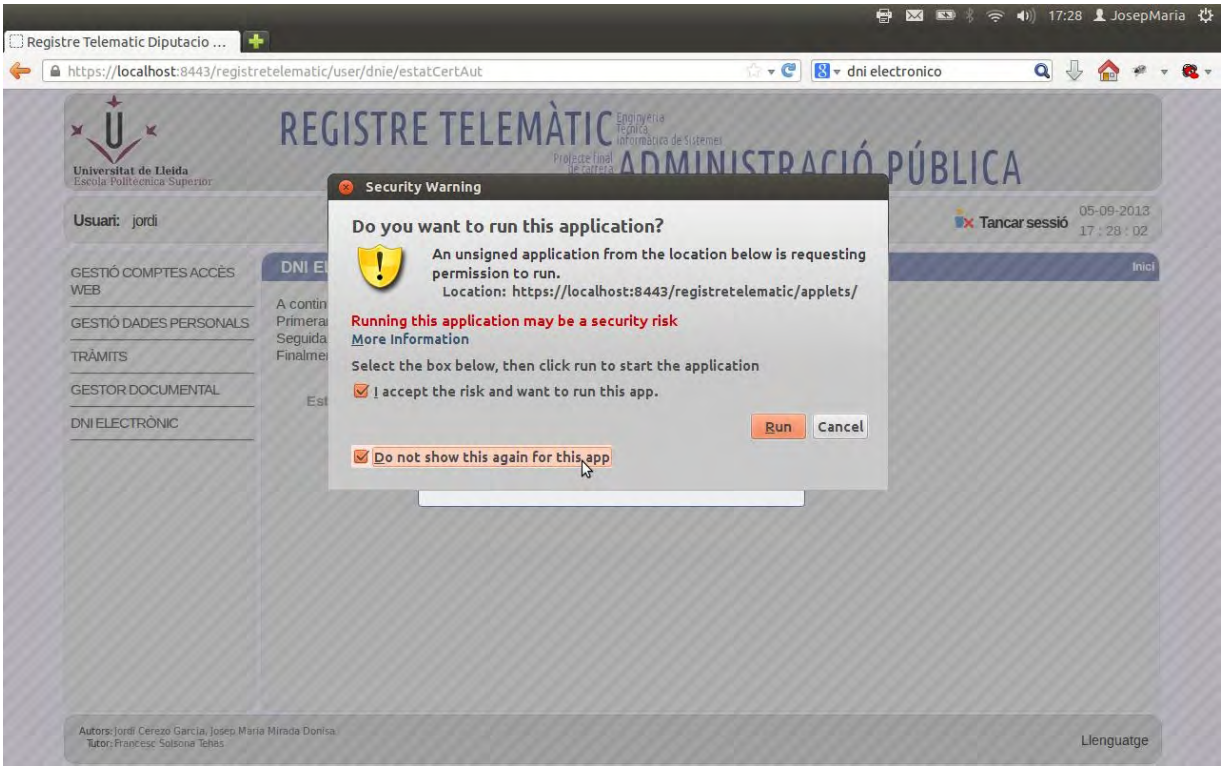
Il·lustració 147: Comprovar estat del certificat. Obtenció estat del certificat.

Java intentarà, seguidament, bloquejar l'execució de l'applet del DNI-e, donat que el considera potencialment perillós. En aquest cas, el ciutadà haurà de negar aquest bloqueig, ja que confia en l'aplicació que l'Administració Pública posa a la seva disposició (Il·lustració 148).



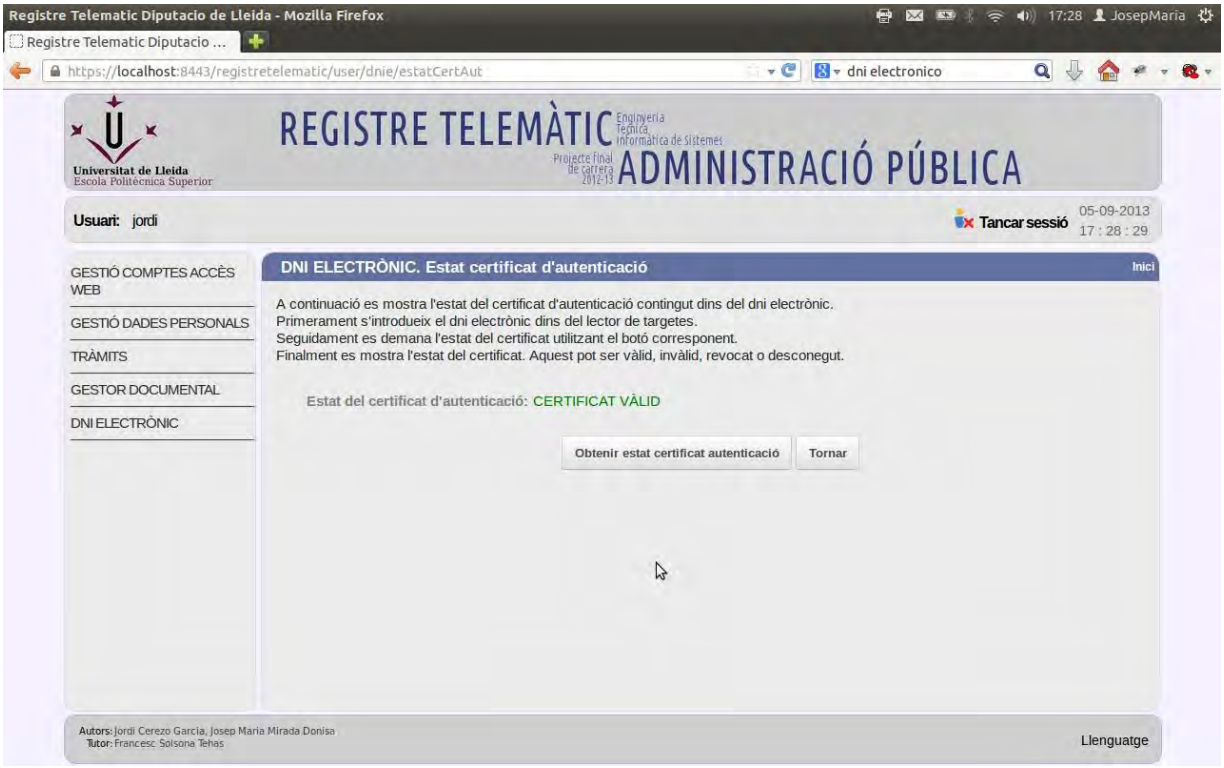
Il·lustració 148: Comprovar estat del certificat. Bloqueig de seguretat.

Per darrera vegada, es demanarà al ciutadà el seu permís per a l'execució de l'applet del DNIe (Il·lustració 149).



Il·lustració 149: Comprovar estat del certificat. Petició permís execució.

Finalment, i si tots els passos s'han realitzat de forma correcta, es mostraran en pantalla un missatge mostrant l'estat del certificat corresponent, és a dir, vàlid o invàlid (Il·lustració 150).

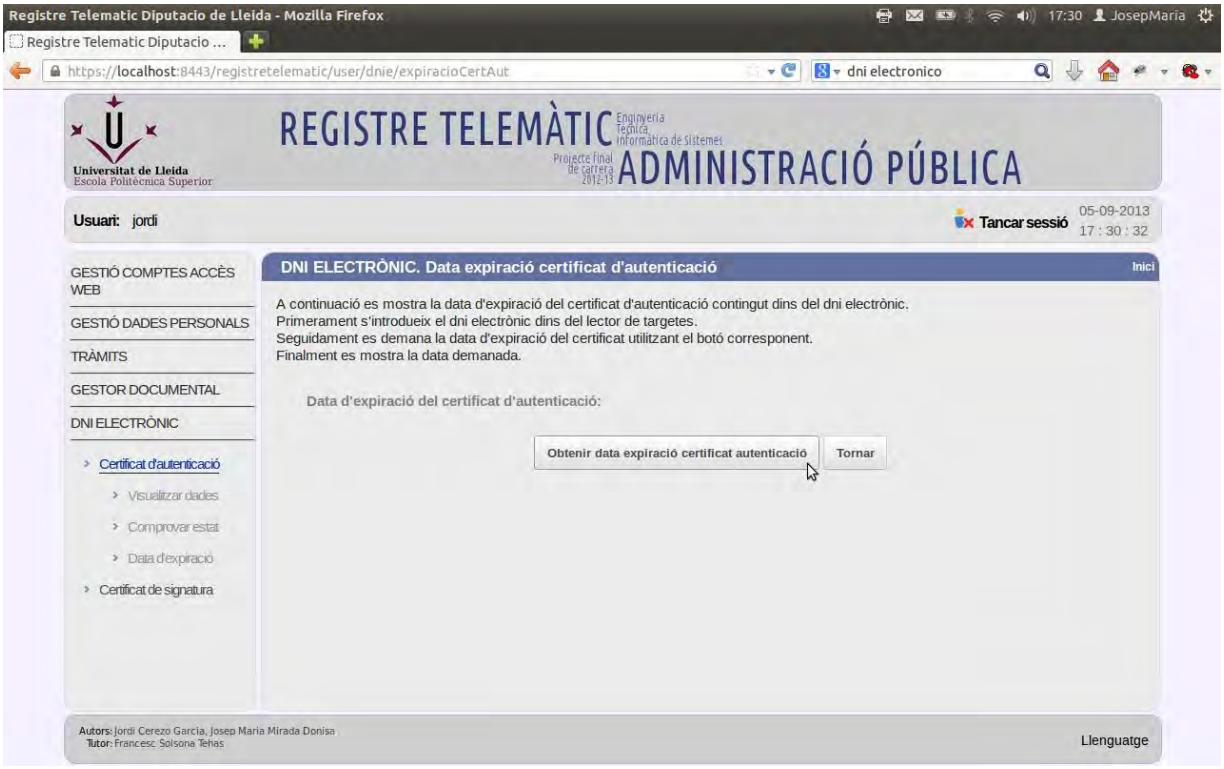


Il·lustració 150: Comprovar estat del certificat. Resultat de la comprovació.

Si qualsevol dels anteriors passos falla, es mostrarà un missatge en pantalla informant sobre l'error.

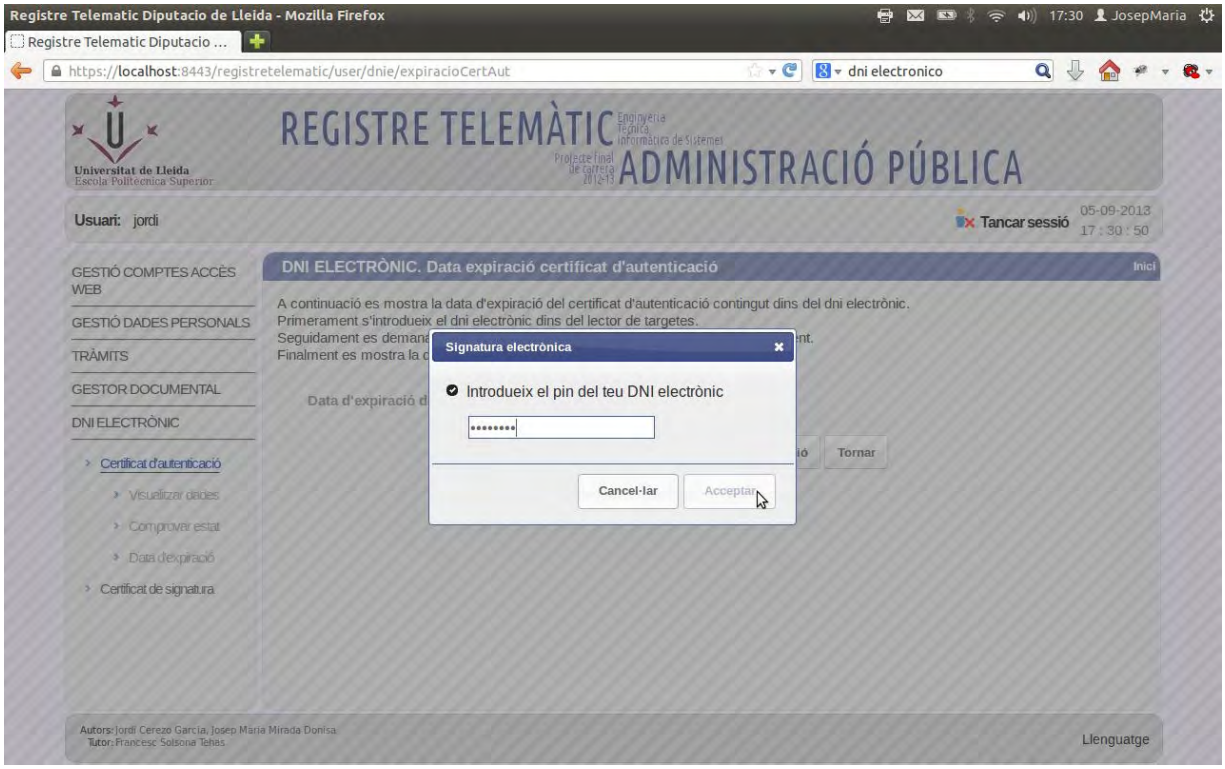
5.3.6.3 Data expiració

En prémer el botó del menú etiquetat com a “Data expiració”, l'aplicació ens dirigirà a la pantalla següent (Il·lustració 151):



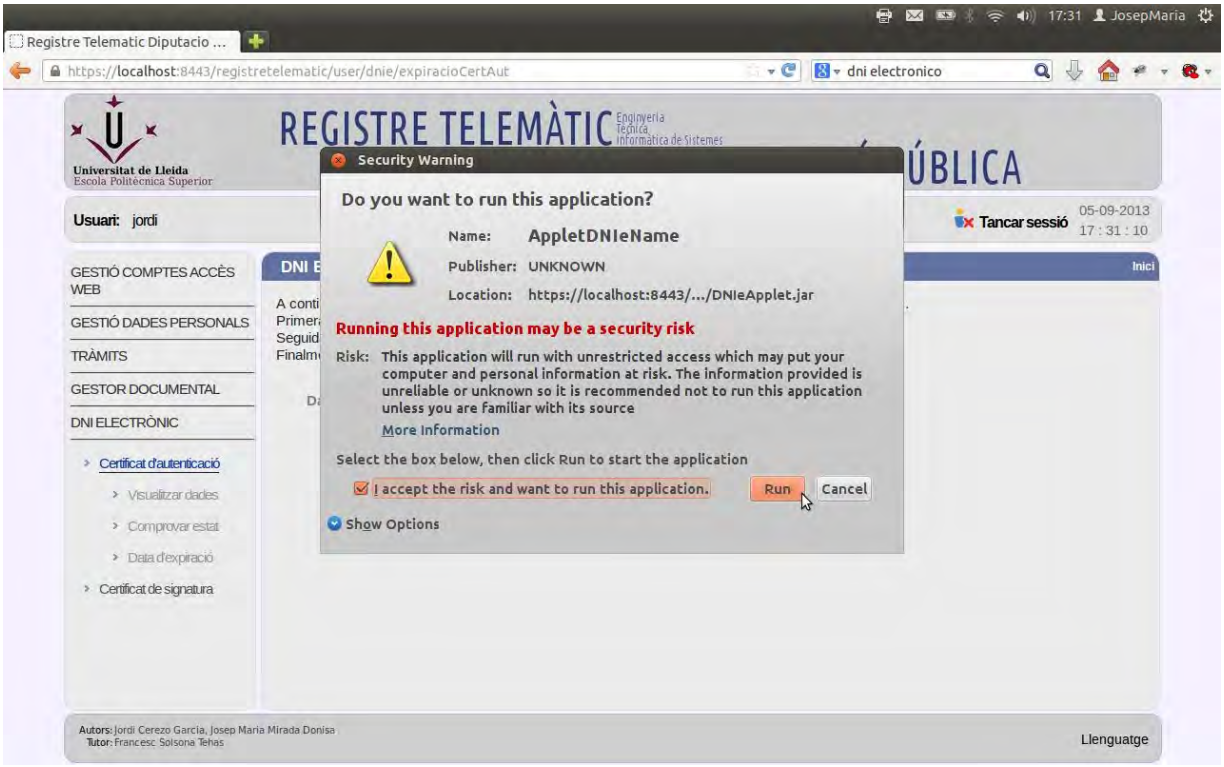
Il·lustració 151: Data d'expiració del certificat. Pantalla inicial.

El ciutadà ha de prémer el botó **"Obtenir data d'expiració del certificat"**, i seguidament l'aplicació demanarà el PIN del DNIe inserit (Il·lustració 157).



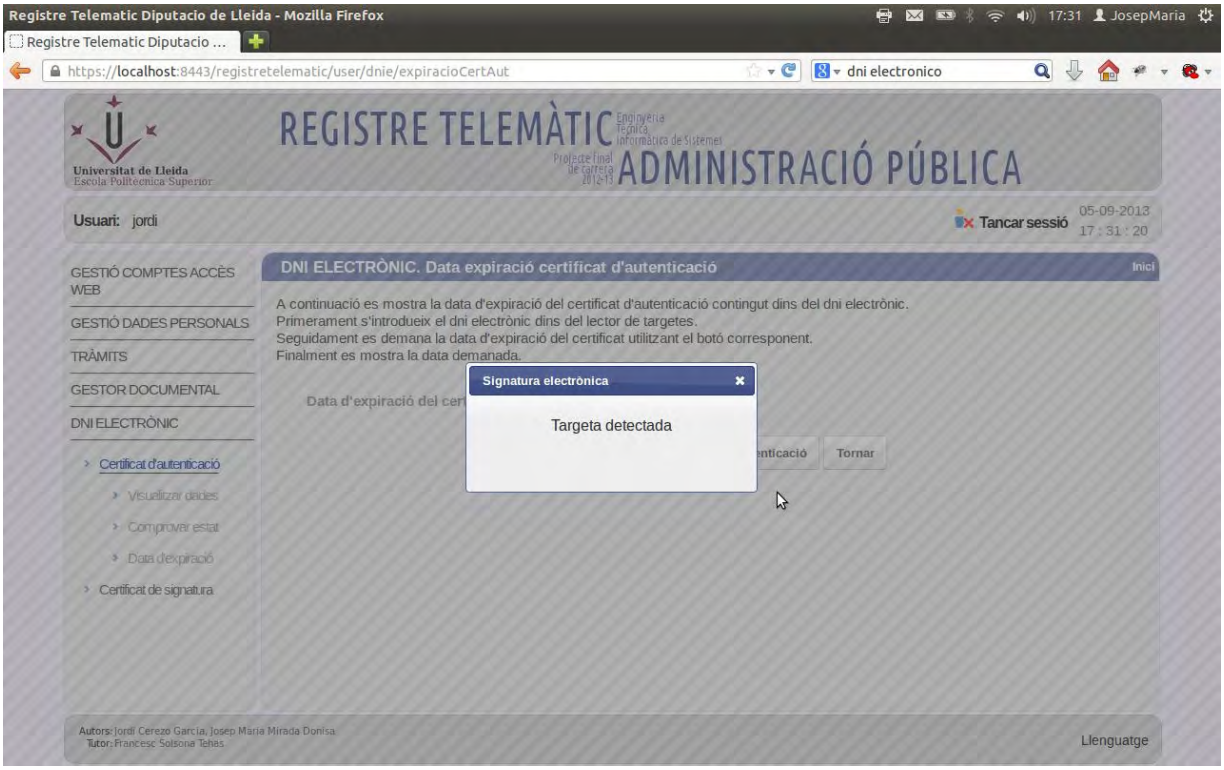
Il·lustració 152: Data d'expiració del certificat. Petició de PIN.

Si el PIN introduït és correcte, l'aplicació ens demanarà permís per a l'execució de l'applet del DNIe (Il·lustració 153):



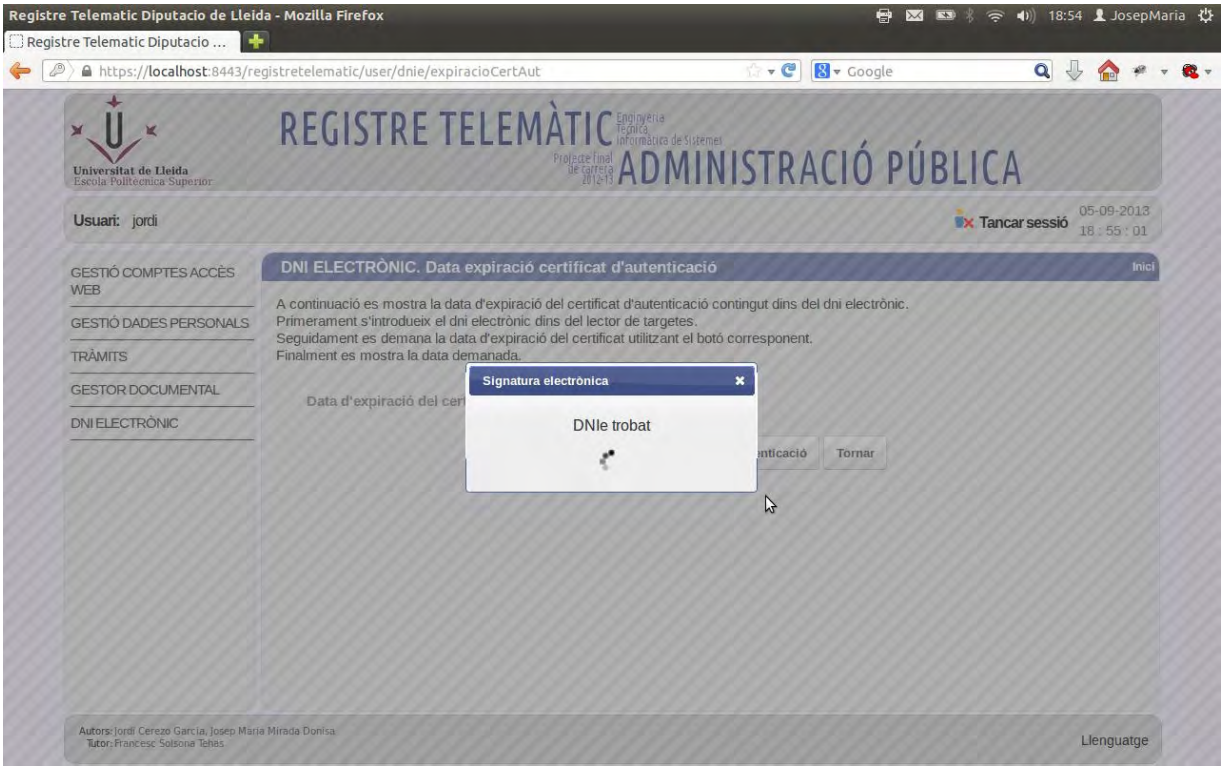
Il·lustració 153: Data d'expiració del certificat. Petició permís d'execució.

El següent pas serà detectar si hi ha una targeta inserida al lector d'smart cards (Il·lustració 154).



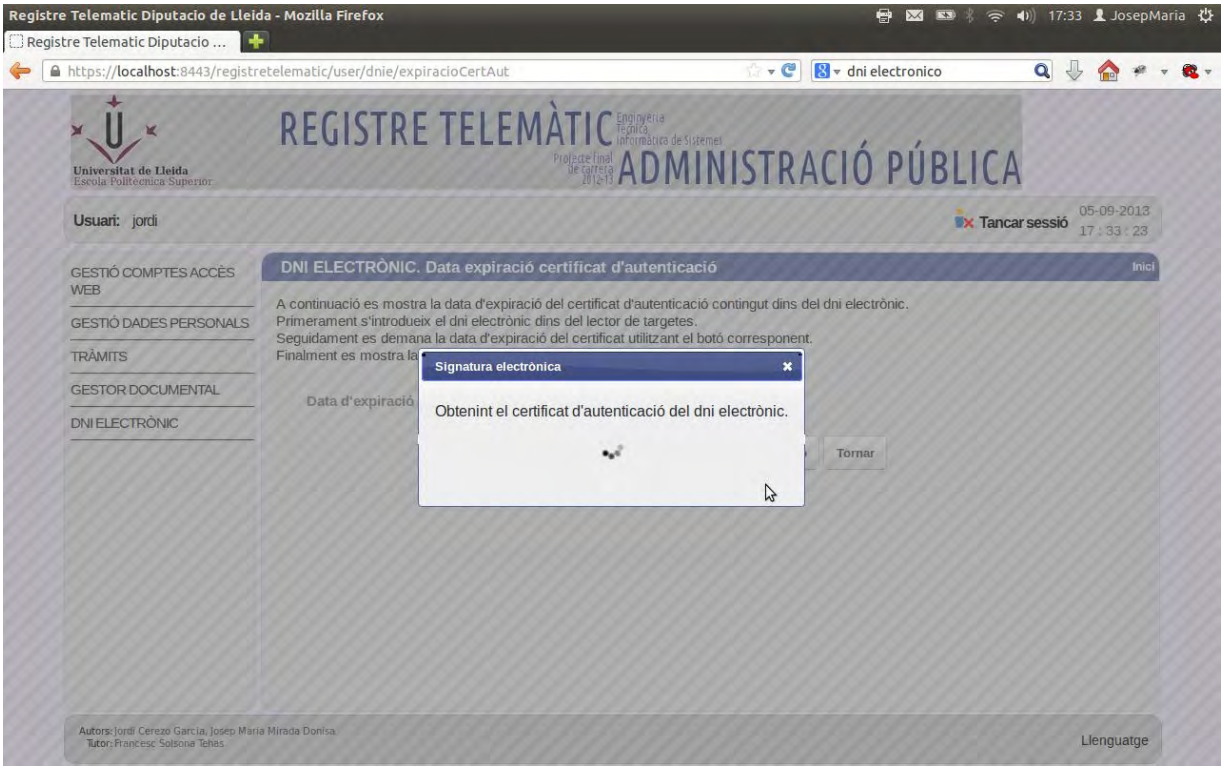
Il·lustració 154: Data d'expiració del certificat. Detecció de targeta.

Si troba una targeta inserida, l'applet detectarà si es tracta d'un DNIe (Il·lustració 155).



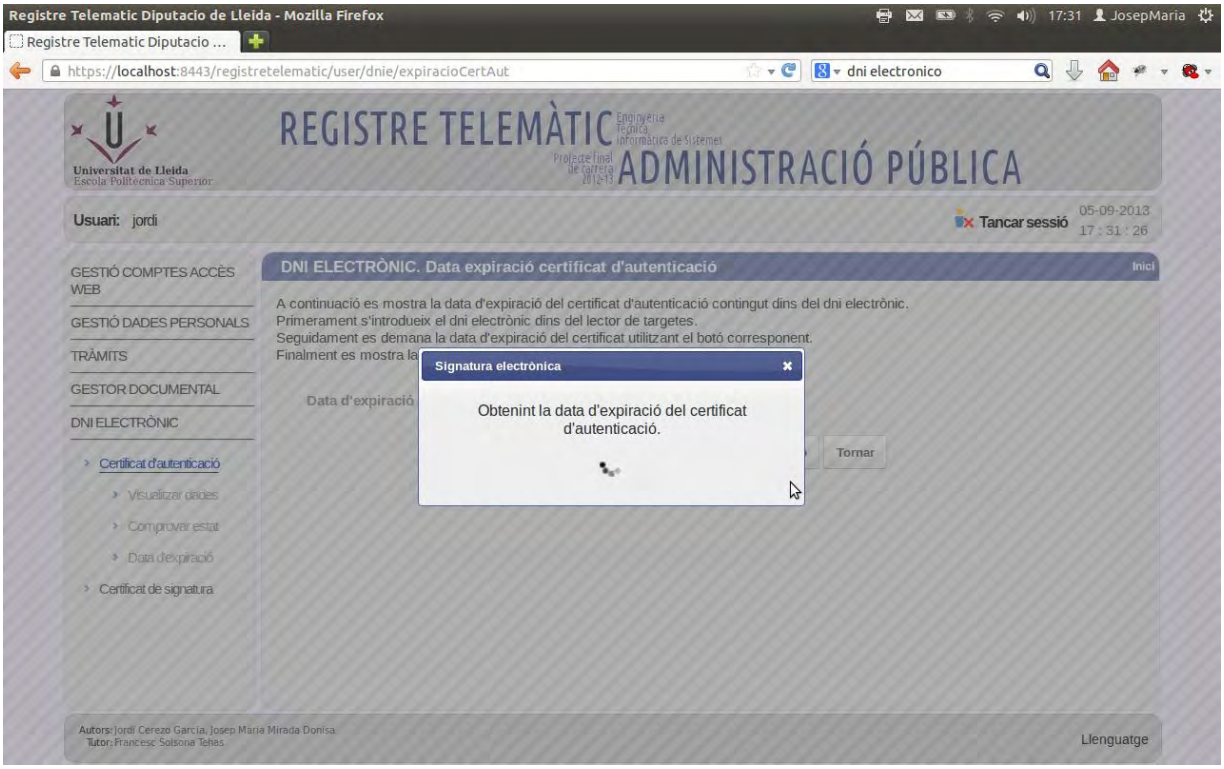
Il·lustració 155: Data d'expiració del certificat. Detecció de DNI-e.

Si la targeta inserida és realment un DNI-e, l'applet n'obtindrà el certificat corresponent, el d'autenticació o signatura segons el cas (Il·lustració 156).



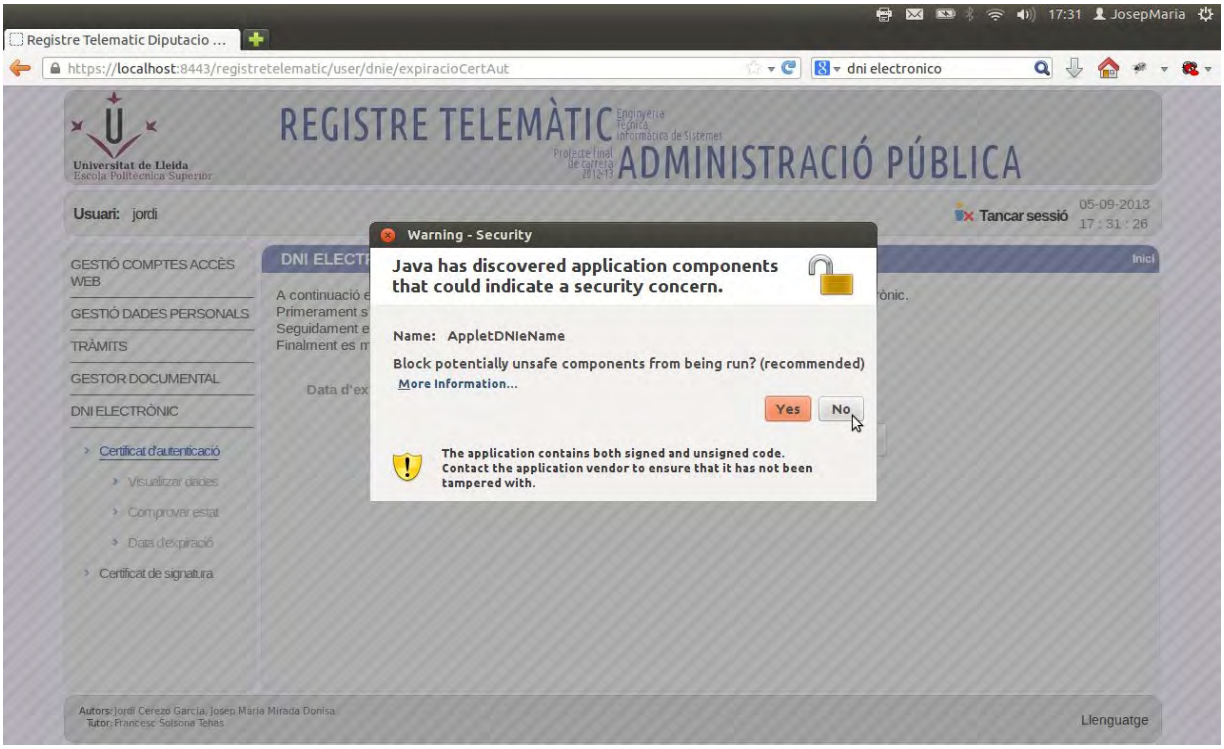
Il·lustració 156: Data d'expiració del certificat. Obtenció del certificat.

El següent pas serà comprovar la data d'expiració del certificat obtingut (Il·lustració 157).



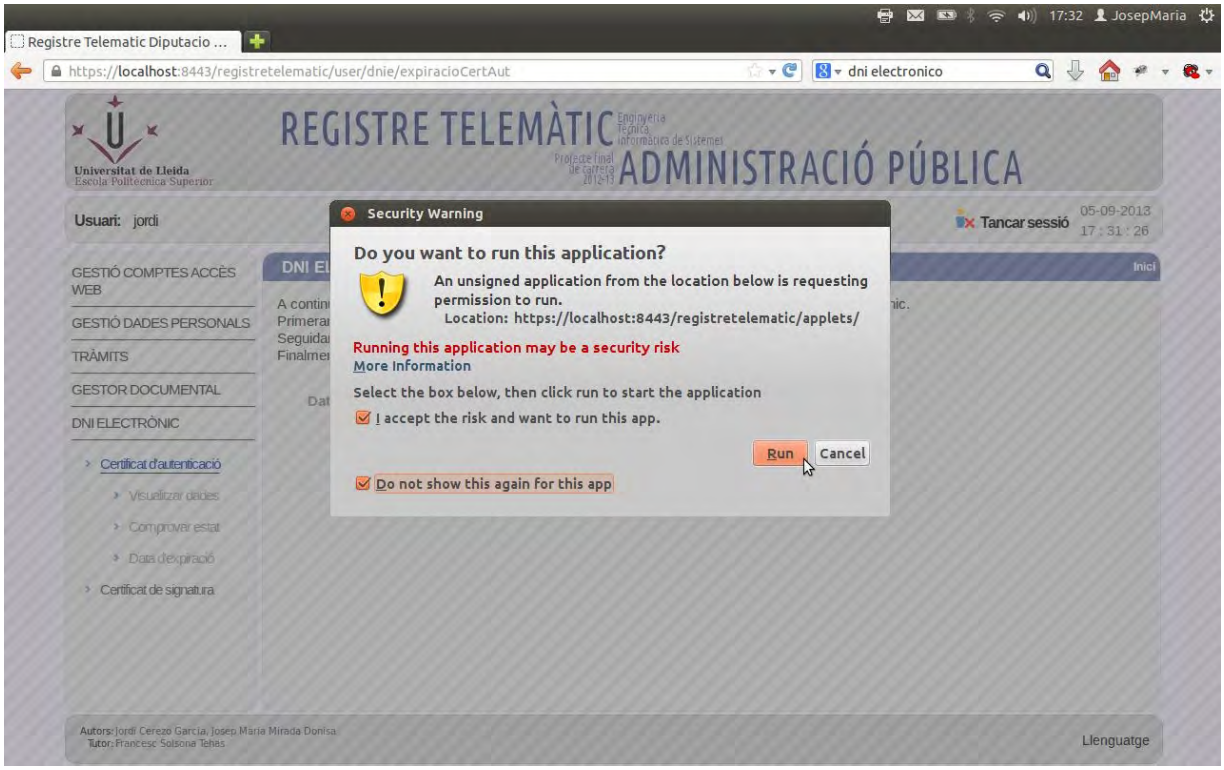
Il·lustració 157: Data d'expiració del certificat. Obtenció de data d'expiració.

Java intentarà, seguidament, bloquejar l'execució de l'applet del DNI-e, donat que el considera potencialment perillós. En aquest cas, el ciutadà haurà de negar aquest bloqueig, ja que confia en l'aplicació que l'Administració Pública posa a la seva disposició (Il·lustració 158).



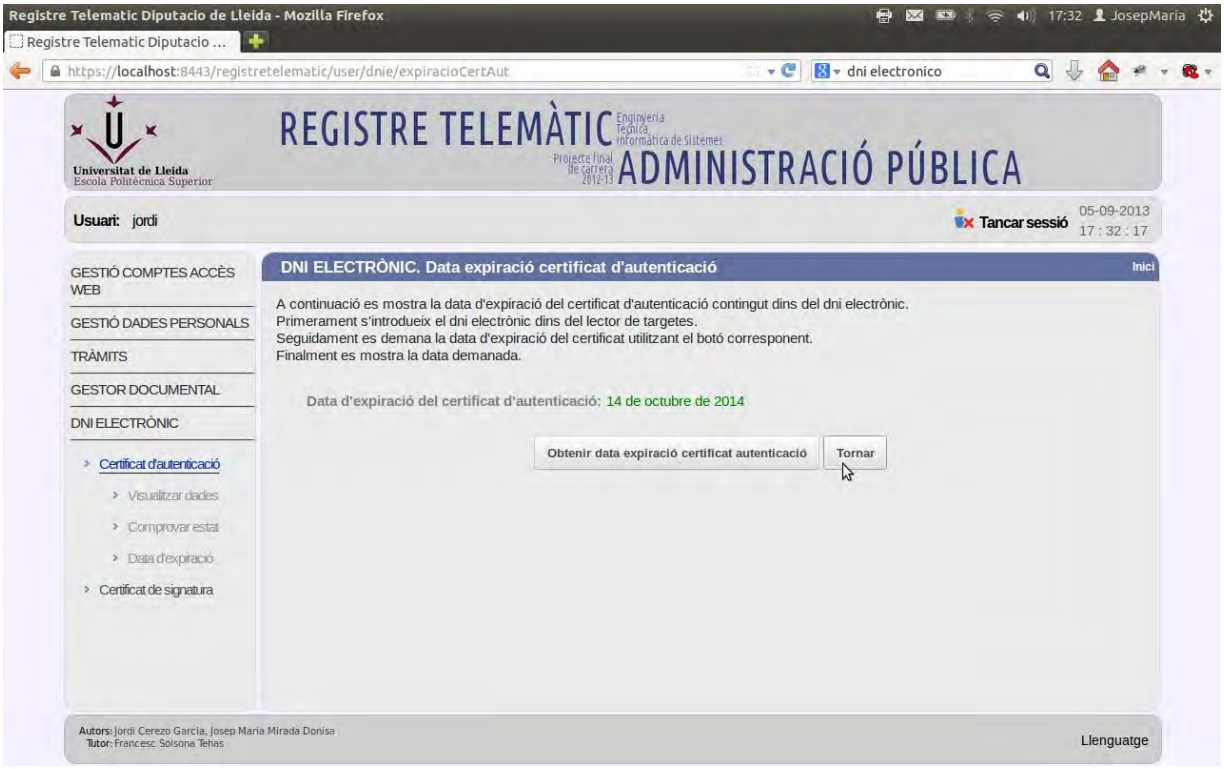
Il·lustració 158: Data d'expiració del certificat. Petició de bloqueig.

Per darrera vegada, es demanarà al ciutadà el seu permís per a l'execució de l'applet del DNIe (Il·lustració 159).



Il·lustració 159: Data d'expiració del certificat. Petició de permís d'execució.

Finalment, i si tots els passos s'han realitzat de forma correcta, es mostraran en pantalla un missatge mostrant l'estat del certificat corresponent, és a dir, vàlid o invàlid (Il·lustració 160).



Il·lustració 160: Data d'expiració del certificat. Obtenció data expiració.

Si qualsevol dels anteriors passos falla, es mostrarà un missatge en pantalla informant sobre l'error.

5.4 Administrador

5.4.1 Pantalla inicial

L'aplicació Registre Telemàtic permet la creació d'un tipus especial d'usuaris, els Administradors. Aquests representen treballadors de l'Administració Pública, que tenen la capacitat de gestionar els comptes d'usuari d'accés a la web, validant les diferents peticions que en aquest àmbit siguin enviades a la base de dades. D'aquesta manera, un administrador serà l'encarregat de donar el vist-i-plau a les altes d'usuari, prèviament revisades per un empleat, a les peticions de bloqueig o desbloqueig de compte per part d'un ciutadà, o a les peticions de desactivació o activació d'un compte per part d'un empleat.

Un administrador validarà el compte d'usuari dels diferents empleats, atorgant-los així la confiança i la capacitat per a la gestió de la resta de possibilitats de l'aplicació web. Les tasques de gestió del dia a dia seran dutes a terme per empleats, però les gestions de comptes d'usuaris restaran en mans dels Administradors.

En connectar-nos a l'aplicació com a Administrador, veurem la seva pàgina inicial (Il·lustració 161), on trobem un menú a la part esquerra, que serà el mètode d'accés a totes les possibilitats que ens proporciona el perfil d'Administrador. Navegant per aquest menú podrem realitzar totes aquelles tasques necessàries per a la gestió de comptes web i dades personals dels diversos usuaris, dades necessàries per al bon funcionament de l'aplicació.

Il·lustració 161: Pantalla de benvinguda de l'Administrador

En aquesta pantalla inicial es mostra un llistat dels esdeveniments que s'han produït a la base de dades respecte als comptes d'accés web, i dades personals dels usuaris de tots els perfils. La primera línia mostra a l'administrador si s'han produït altes de comptes web per part dels empleats. La

segona i tercera línia mostren si s'han produït peticions de bloqueig o desbloqueig de comptes per part dels usuaris, és a dir, dels ciutadans. Les dues darreres línies mostren les peticions de activació i desactivació de comptes per part dels empleats de l'Administració. En tots els casos, l'Administrador podrà veure el nombre de peticions de cada tipus rebudes, i dirigir-se a la pantalla corresponent per tal de validar, o no validar, el canvi. Mentre una petició no sigui validada per un administrador, aquesta no tindrà efecte.

Passem, tot seguit, a veure les capacitats que conté el menú lateral per al perfil d'usuari “Administrador”.

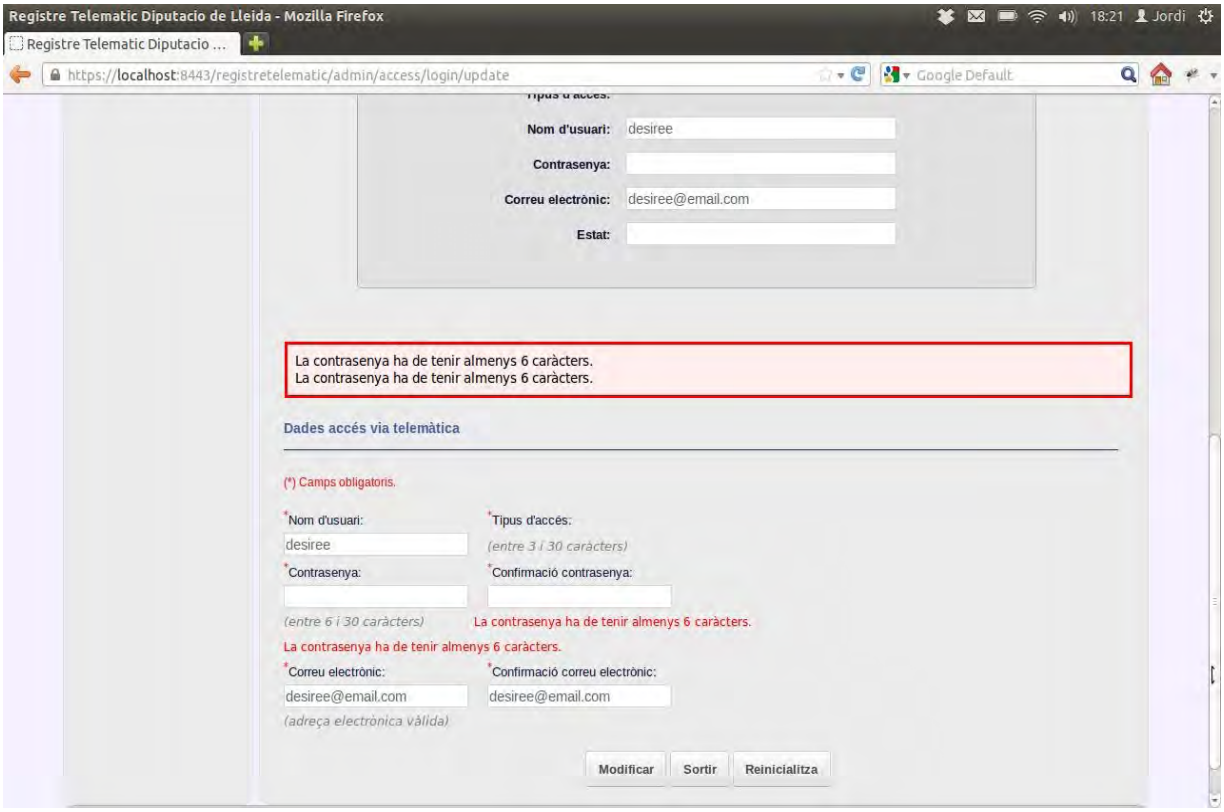
5.4.2 Gestió de comptes d'accés web

La primera entrada del menú lateral (Il·lustració 162), ens permetrà la **“Gestió dels comptes d'accés a la web”** del programa, és a dir, la gestió dels comptes d'usuaris que tenen accés a l'aplicació. En el cas de l'Administrador, el seu paper no serà la creació o manteniment de comptes, si no la validació dels comptes introduïts prèviament pels empleats. En prémer aquest botó, es desplegarà el menú associat amb una sèrie d'entrades que ens faciliten aquestes validacions. Tot seguit passem a veure-les més detalladament.

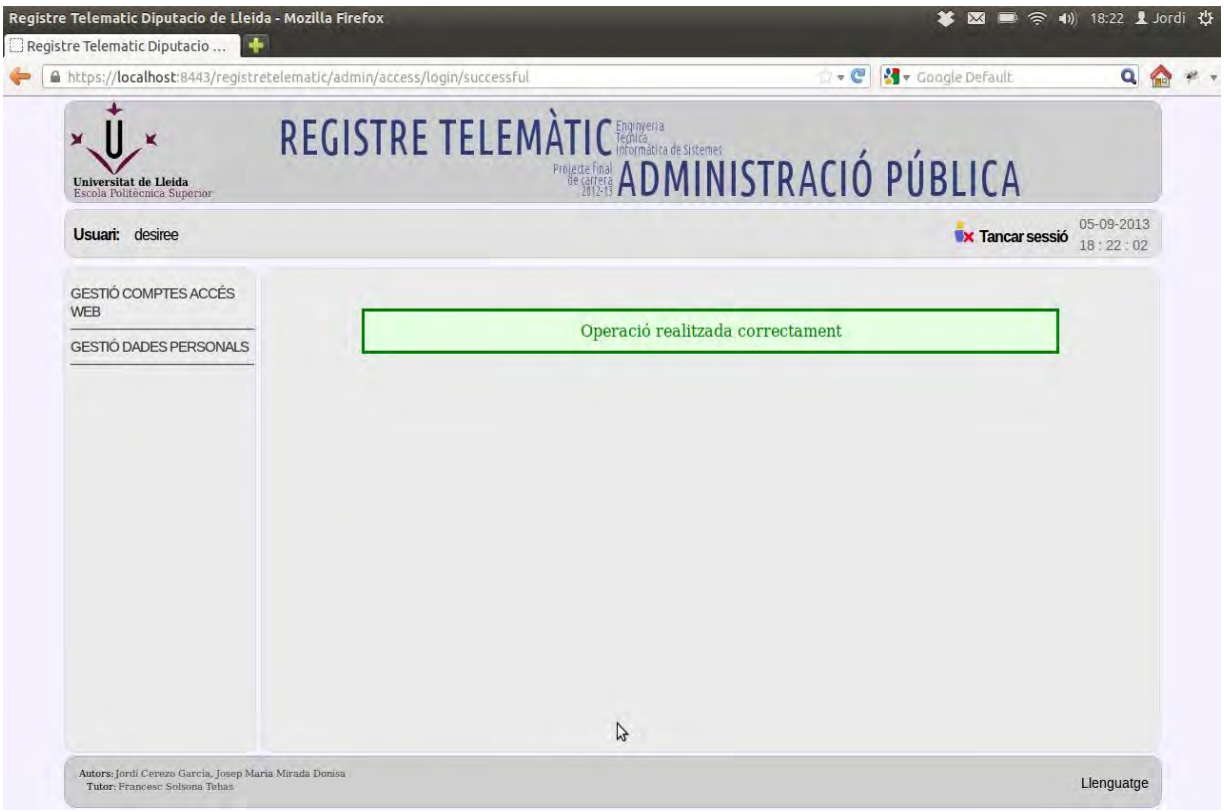
Il·lustració 162: Gestió de comptes d'accés web, validació de l'Administrador

5.4.2.1 El meu compte d'accés web

En prémer aquest botó, es desplegaran dues noves opcions en pantalla. La primera, etiquetada com **“Consultar i modificar el meu nom d'usuari i contrasenya”**, permetrà a l'administrador la consulta i modificació de les dades del seu compte d'accés a la pàgina web. A la part superior es mostren les dades de la persona associada al compte web, i a la part inferior, les dades del compte d'accés. Aquestes són les dades que poden ser alterades. Per tal de fer-ho, s'han d'escriure les noves dades a les caixes de text, i prémer el botó **“Modificar”**. Si les dades són incorrectes, es mostrarà un missatge d'error a la vora de les caixes de text on s'ha detectat l'error informant a l'usuari del problema (Il·lustració 163). Si les dades no presenten cap error, es mostrarà un missatge informant de la correcta modificació (Il·lustració 164).

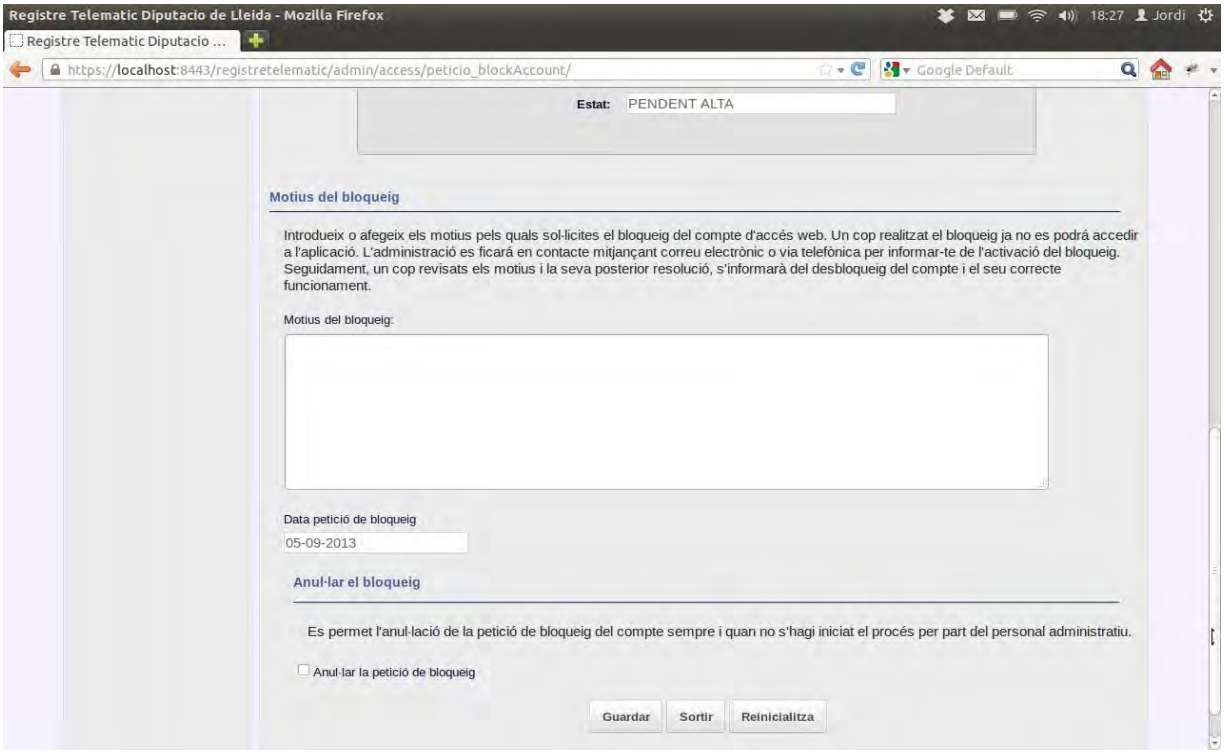


Il·lustració 163: Gestió del meu compte web d'administrador mostrant un error a les dades



Il·lustració 164: Gestió del meu compte web d'administrador mostrant l'èxit en la operació

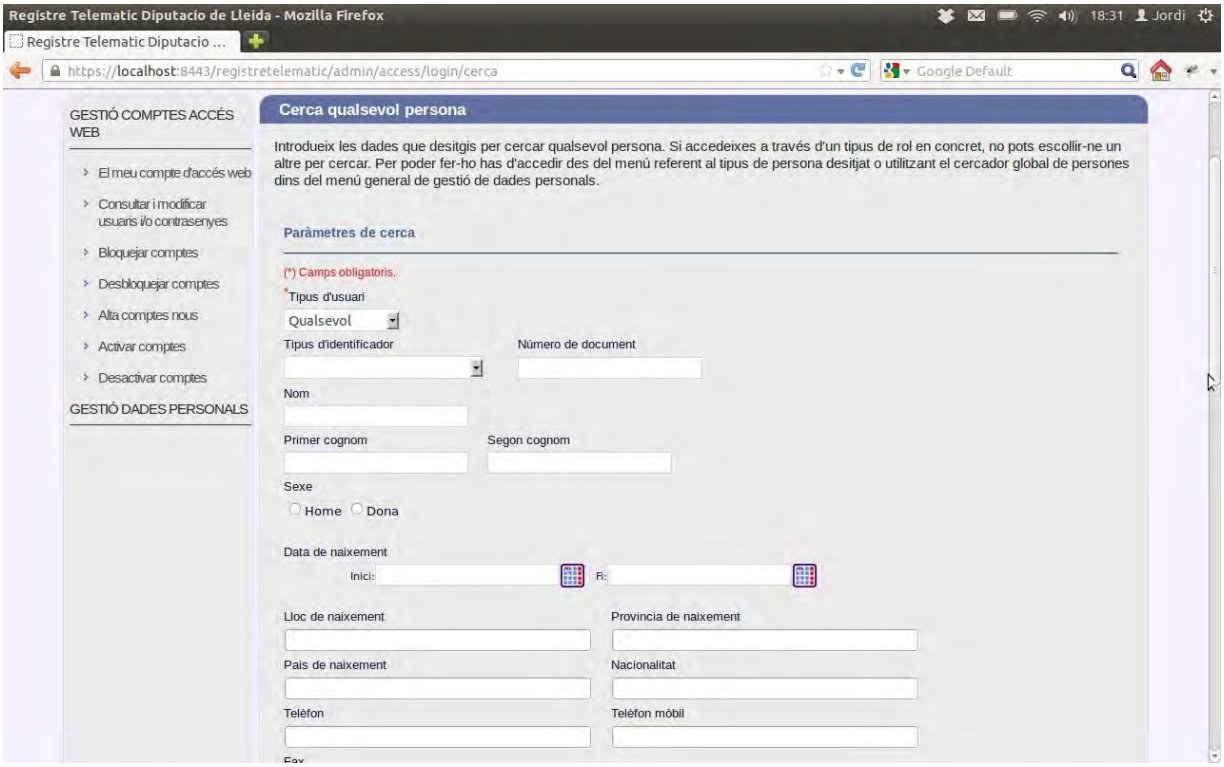
El segon botó etiquetat com a **“Bloquejar el meu compte”** permet bloquejar el propi compte de l'administrador que ha iniciat sessió a l'aplicació (Il·lustració 165). A la part inferior de la pantalla es demanen els motius pels quals es vol donar de baixa el compte, cosa que es realitza prement el botó “Guardar”. També és visible un checkbox que permet, activant-lo, anul·lar una petició de bloqueig, sempre que el procés no hagi estat iniciat pel personal administratiu de l'Administració.



Il·lustració 165: Bloqueig del propi compte de l'administrador

5.4.2.2 Consultar i modificar usuaris i/o contrasenyes

El segon botó del menú de **"Gestió de comptes d'accés web"** ens adreça directament a un cercador de persones (Il·lustració 166), els quals es troben a la base de dades de l'aplicació.



Il·lustració 166: Cercador de persones per consultar i modificar i validar comptes d'accés web

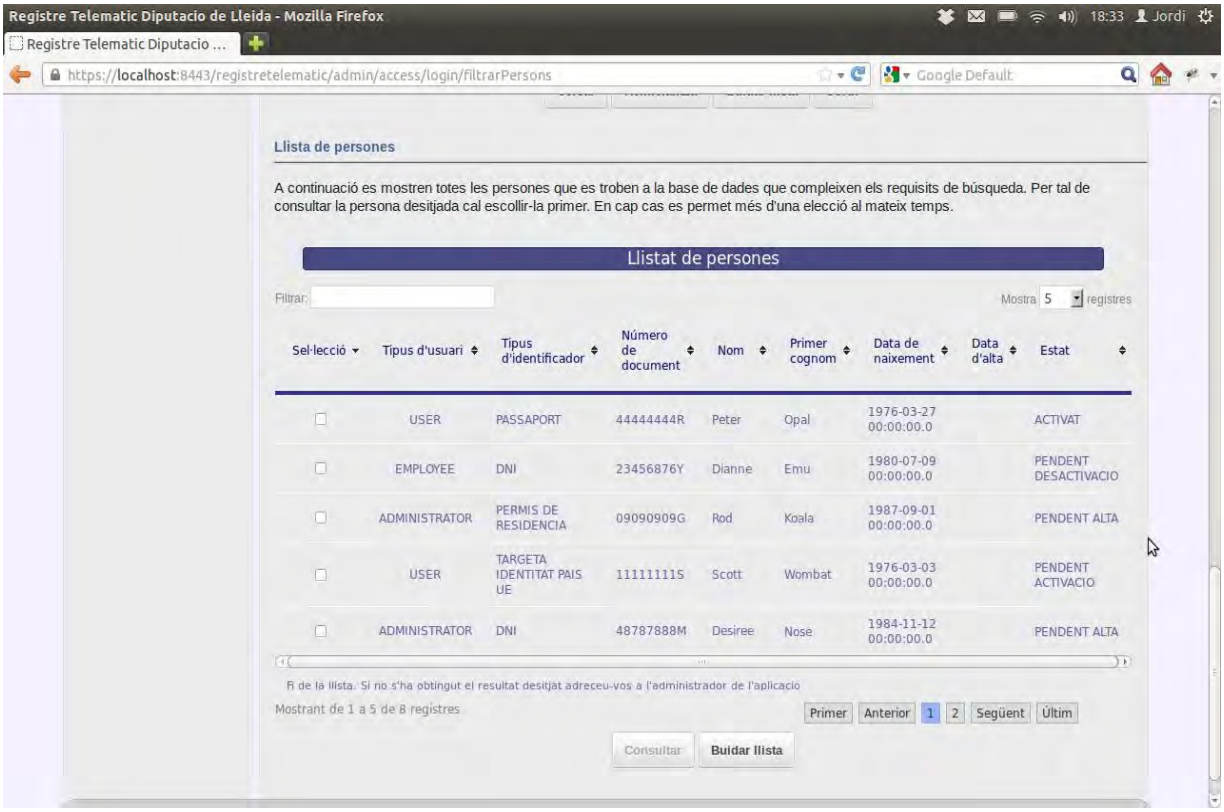
Aquesta pàgina permet realitzar una cerca de persones, filtrant els resultats per tots aquells paràmetres que es troben en pantalla, i mostrant els resultats a la taula de la part inferior:

- **Tipus d'usuari**: permet escollir el tipus d'usuari a cercar, administrador, empleat o usuari. Si es deixa en “Qualsevol”, es cercarà per tots els tipus d'usuari.
- **Tipus d'identificador/Número de document**: permet triar el tipus de document mitjançant el qual la persona es va identificar per donar-se d'alta a l'aplicació, i el número d'aquest document.
- **Nom i cognoms**: permet cercar segons el nom i cognoms de l'usuari. La cerca es realitza per comparació de cadenes de text, de tal manera que, si només coneixem una part del nom, podem escriure només aquella part, i l'aplicació cercarà els usuaris que continguin aquella part.
- **Sexe**: segons si és home o dona. Si no es marca un dels dos, aquest paràmetre no es tindrà en compte (es mostraran els usuaris d'ambdós sexes).
- **Data de naixement**: l'aplicació permet acotar la data de naixement a dues dates concretes. Si no s'emplenen aquests camps, el paràmetre no es tindrà en compte. Si només es plena la data d'inicial, es mostraran les persones amb data de naixement posterior a la introduïda. Si només es plena la data final, es mostraran les persones amb data de naixement anterior a la introduïda.
- **Lloc de naixement**: permet buscar persones nascudes a una localitat concreta.
- **Província de naixement**: permet buscar persones nascudes a una província concreta.
- **País de naixement**: permet buscar persones nascudes a un país concret.
- **Nacionalitat**: permet buscar persones d'una nacionalitat concreta.
- **Telèfon**: permet buscar persones segons el seu telèfon.
- **Telèfon mòbil**: permet buscar persones segons el seu telèfon mòbil.
- **Fax**: permet buscar persones segons el seu fax.
- **Clau d'accés web**: permet cercar segons la seva contrasenya.
- **Estat**: permet cercar segons l'estat del compte a la base de dades.

És possible també realitzar una ordenació dels resultats segons qualsevol dels paràmetres presents al desplegable “Ordenat per:”, i disposar-los de manera ascendent o descendent. Per realitzar la cerca, s'ha de prémer el botó **“Cercar”**. El botó **“Reinicialitza”** restaura tots els camps del cercador al seu estat per defecte. El botó **“Buidar llista”** permet buidar la llista de la taula inferior, corresponent a la darrera cerca realitzada. El botó **“Sortir”** ens porta directament a la pantalla inicial de l'aplicació.

La llista de la part inferior de la pantalla contindrà, com s'ha esmentat anteriorment, els resultats de la la darrera cerca realitzada (Il·lustració 167). Aquesta taula té diverses funcionalitats pròpies. A la part superior esquerra hi ha una caixa de text mitjançant la qual es poden filtrar els resultats de la taula, amb la finalitat d'afinar encara més la cerca. A la part superior dreta es pot introduir el número de registres que es volen mostrar a cada pàgina de la taula. A la part inferior dreta hi ha una sèrie de botons que permeten la navegació a través dels registres de la taula, portant a l'usuari de forma

directa a la primera pàgina, la pàgina anterior, la pàgina següent, la pàgina final, i qualsevol d'elles de manera directa, mitjançant el seu número. ***Totes les taules de resultats de l'aplicació tenen la mateixa funcionalitat, per tant, en totes les pantalles que mostrin un llistat d'ara en endavant en aquest document, obviarem l'explicació del funcionament de la taula, i la navegació pels registres mostrats.***

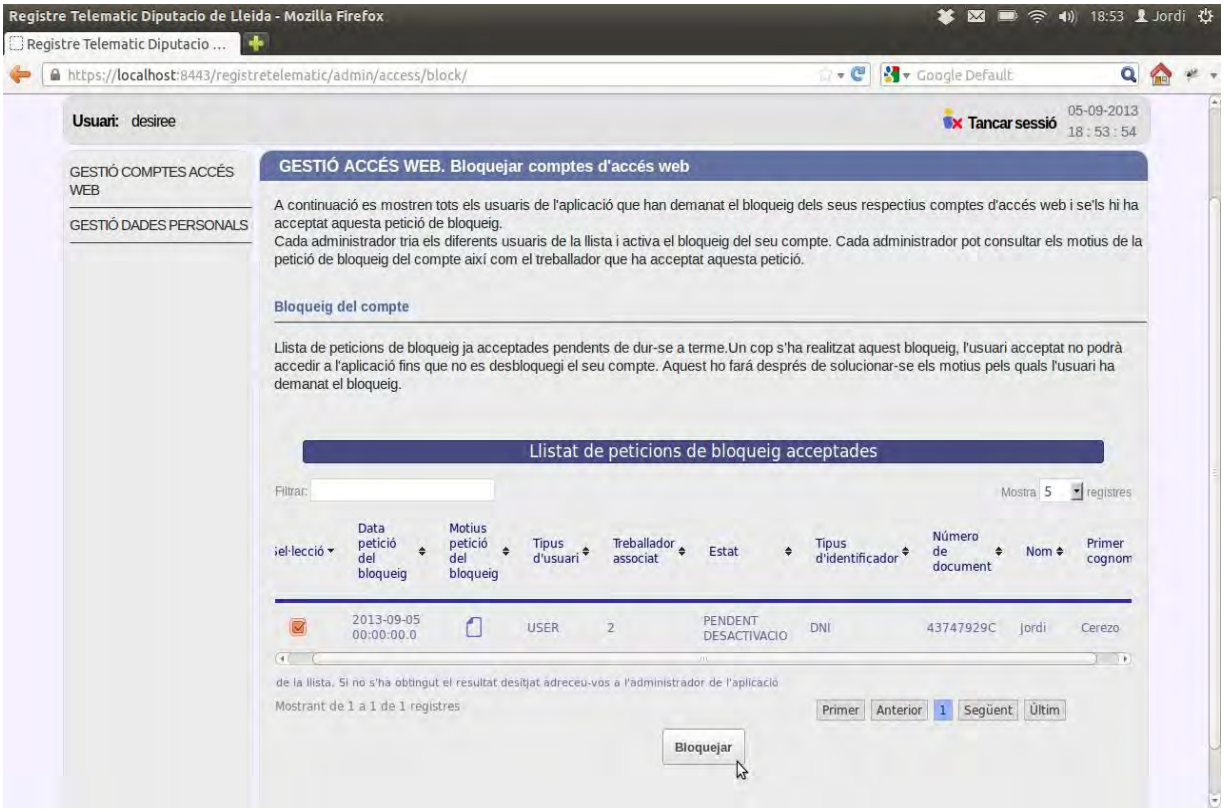


Il·lustració 167: Llistat de resultat del cercador de comptes web per a l'adminsistrador

Un cop la taula contingui resultats, l'empleat pot seleccionar qualsevol dels usuaris, i un cop fet, prémer el botó **"Consultar"**. Mitjançant aquests passos, s'obrirà la pàgina de consulta i modificació del compte d'usuari seleccionat, on les dades podran ser alterades. Anàlogament a la modificació del compte del propi administrador que ha iniciat sessió, si les dades introduïdes són incorrectes, es mostrarà un missatge d'error a la vora de la dada errònia. Si les dades són correctes, es mostrarà una pantalla informant de modificació correcta de les dades.

5.4.2.3 Bloquejar comptes d'usuaris

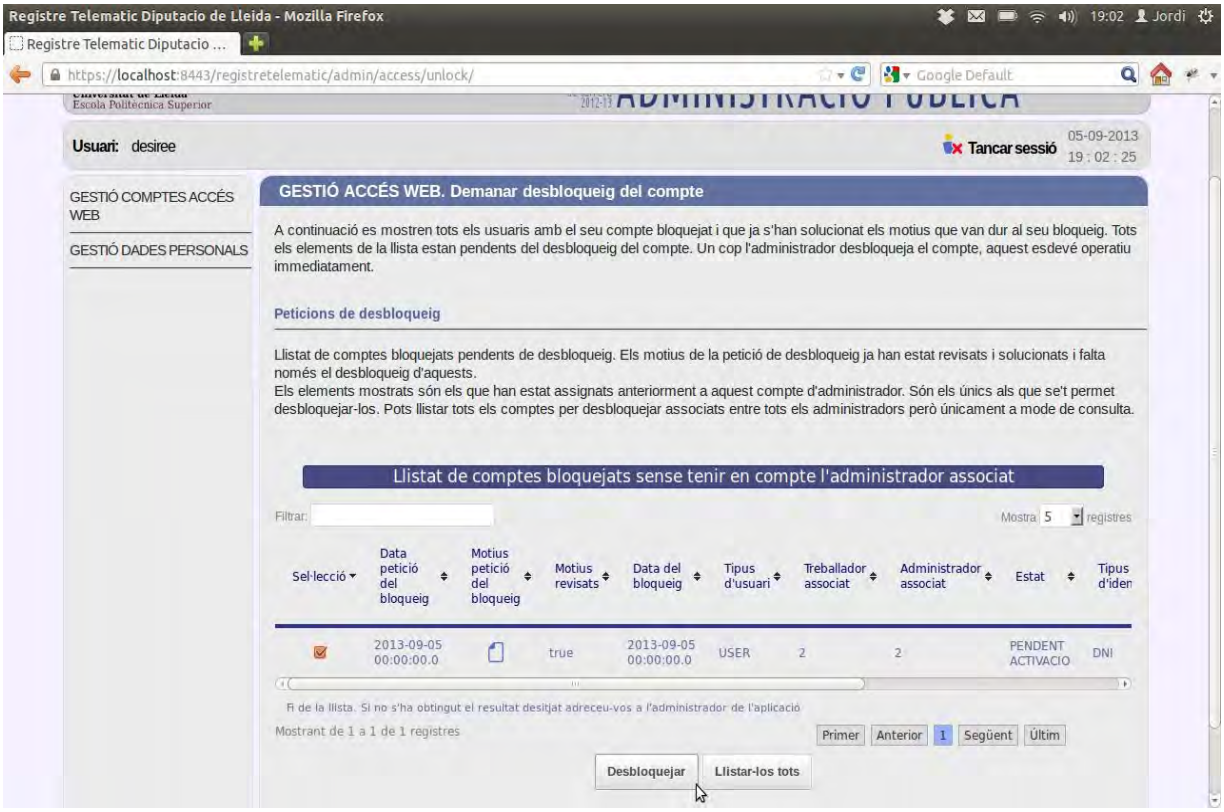
La següent entrada del menú de comptes d'usuaris és la etiquetada com a **"Bloquejar comptes d'usuari"**. En prémer aquest enllaç, l'administrador serà adreçat a una pàgina on es llisten totes les **peticions de bloqueig de comptes que han estat acceptades prèviament per un usuari de tipus "Empleat"**, a la taula de la part inferior (Il·lustració 168). L'administrador pot comprovar els motius adduïts per demanar el bloqueig del compte, i si els troba coherents, pot marcar la petició de bloqueig referida, i bloquejar-la prement el botó **"Bloquejar"**. En qualsevol cas, la resolució de la petició de bloqueig haurà de ser notificada a l'usuari via telefònica, o bé a través de correu electrònic. D'aquesta manera, el bloqueig realment ha estat validat per un usuari "Administrador".



Il·lustració 168: Validació de bloqueig de comptes d'usuari

5.4.2.4 Desbloquejar comptes d'usuaris

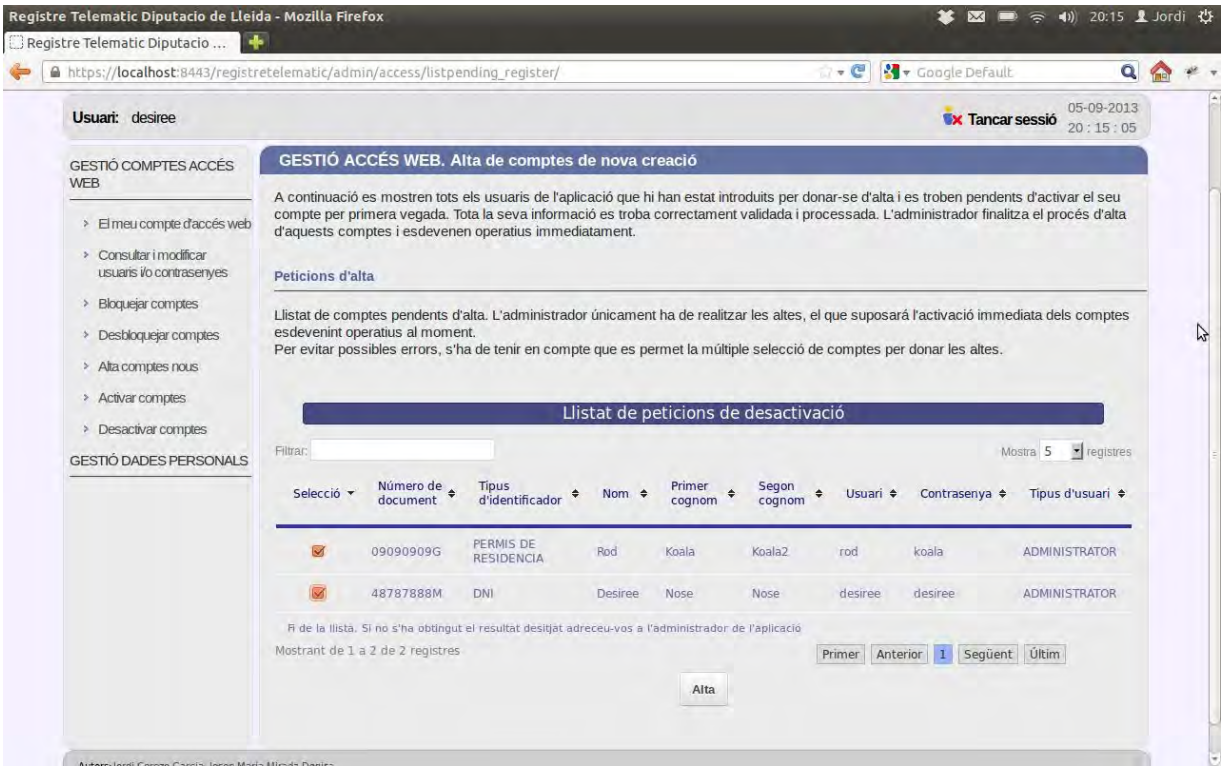
L'entrada del menú etiquetada com a **"Desbloquejar comptes d'usuari"**, adreçarà l'administrador a una pàgina on es llisten totes les peticions de desbloqueig de comptes validades per un usuari de tipus **"Empleat"**. Seran mostrats a la taula de la part inferior (Il·lustració 169). L'administrador pot marcar a la taula una de les peticions de desbloqueig, i, prement el botó **"Desbloquejar"**, retornar-li la seva funcionalitat original. L'administrador només podrà desbloquejar aquells comptes web que van ser prèviament bloquejats per ell, i que són els mostrats per defecte a la llista. Això és degut a que, donat que aquest administrador és qui ha llegit i valorat els motius per validar la petició de bloqueig, ha de ser ell mateix, i no un altre administrador, qui decideixi si els motius de bloqueig han cessat. Existeix la possibilitat, però, de consultar totes les peticions de bloqueig de l'aplicació, encara que fossin validades per un altre administrador. Per fer-ho, s'ha de prémer el botó **"Llistar-los tots"** de la part inferior de la pantalla. Per tornar a mostrar només les peticions de desbloqueig de l'administrador connectat, s'ha de prémer el mateix botó, etiquetat ara com a **"Llistar els propis"**. El compte d'usuari desbloquejat passarà a gaudir de la mateixa funcionalitat que tenia originalment.



Il·lustració 169: Desbloquejar comptes d'usuari per part de l'administrador

5.4.2.5 Alta de comptes nous

El següent botó de la gestió de comptes web, està etiquetat com a **“Alta comptes nous”**. En pantalla es mostrarà una taula que conté un llistat dels comptes d'usuari de nova creació, introduïts pels empleats de l'Administració (Il·lustració 171). L'administrador triarà, mitjançant el checkbox de selecció, quins dels nous comptes d'usuari vol validar (cal remarcar que en aquest cas, i per agilitzar la validació dels comptes, es permet la selecció múltiple). Prement el botó inferior etiquetat com a **“Alta”**, l'administrador donarà el vist-i-plau als nous comptes d'usuari, atorgant-los la capacitat d'accés a l'aplicació web.



Il·lustració 170: Alta de comptes web per part de l'administrador

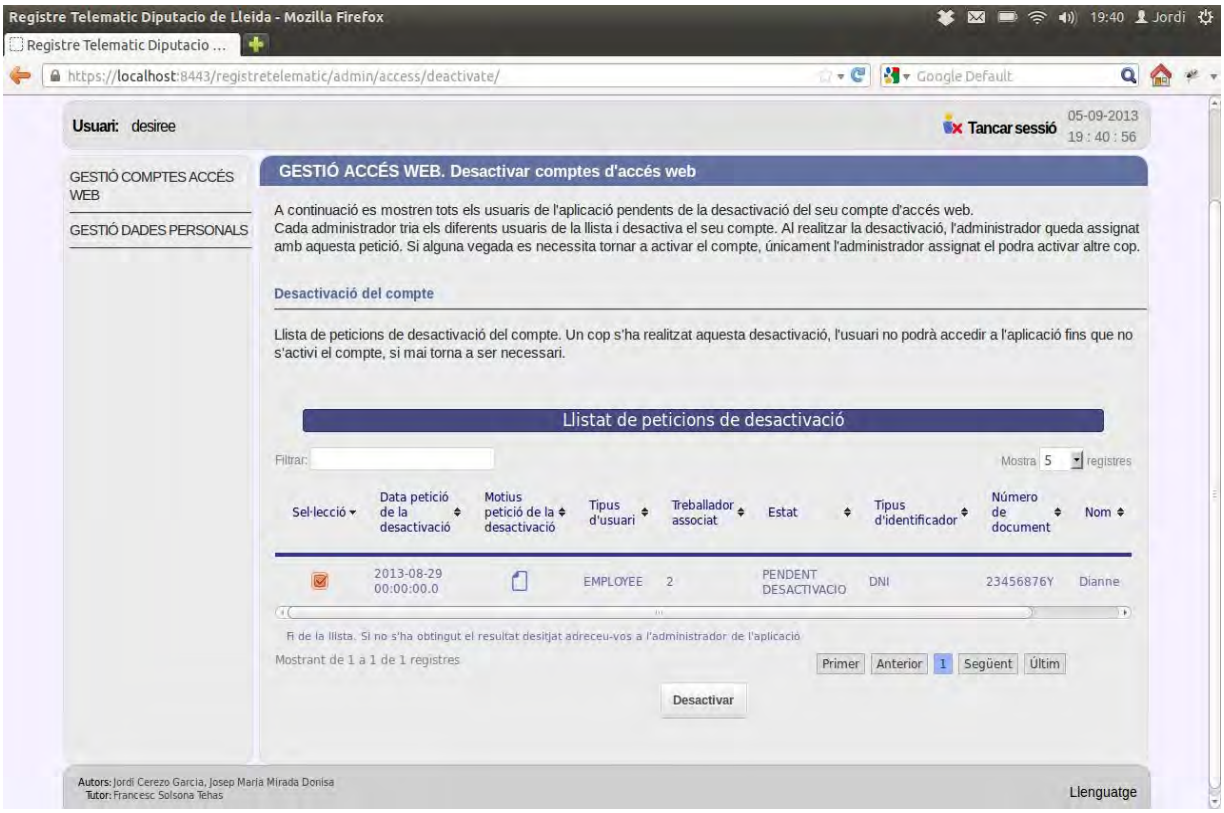
5.4.2.6 Activar comptes d'usuaris

La següent entrada del menú de comptes d'usuaris és la etiquetada com a **"Activar comptes d'usuari"**. En prémer aquest enllaç, l'administrador serà adreçat a una pàgina on es llisten els comptes d'usuari que han estat desactivats per ell, mitjançant una taula que es troba a la part inferior de la pàgina i que disposa de diverses funcionalitats pròpies (Il·lustració 171). A la part superior esquerra de la taula hi ha una caixa de text mitjançant la qual es poden filtrar els resultats, amb la finalitat d'afinar encara més la cerca. A la part superior dreta es pot introduir el número de registres que es volen mostrar a cada pàgina de la taula. A la part inferior dreta hi ha una sèrie de botons que permeten la navegació a través dels registres de la taula, portant a l'usuari de forma directa a la primera pàgina, la pàgina anterior, la pàgina següent, la pàgina final, i qualsevol d'elles de manera directa, mitjançant el seu número. L'administrador pot comprovar els motius adduïts per un empleat per demanar la reactivació d'un compte prèviament desactivat, i si els troba coherents, pot marcar el checkbox de la petició d'activació referida, i prémer el botó **"Activar"**. L'administrador només pot reactivar els comptes d'usuari que van ser desactivats per ell, i que seran els que es mostren per defecte a la taula d'aquesta pantalla. Això és degut a que aquest aquest administrador és qui coneix els motius de la petició de desactivació, i per tant, ha de ser ell qui valori si aquests motius han cessat. Existeix la possibilitat, però, de consultar tots els comptes desactivats de l'aplicació, encara que fossin desactivats per a altres administradors. Per fer-ho, s'ha de prémer el botó **"Llistar-los tots"** de la part inferior de la pantalla. Per tornar a mostrar només els les peticions assignades a l'administrador que ha iniciat sessió, s'ha de prémer el mateix botó, etiquetat ara com a **"Llistar els propis"**.

Il·lustració 171: Activació de comptes per part de l'administrador

5.4.2.7 Desactivar comptes d'usuari

El darrer botó del menú de **"Gestió de comptes d'accés web"** ens adreça directament a u una pantalla on es llisten totes les peticions de desactivació de comptes web realitzades pels empleats mitjançant una taula a la part inferior.



Il·lustració 172: Llistat de peticions de desactivació de comptes

L'administrador pot comprovar el motius pels quals un empleat ha realitzat la petició de desactivació. Si els troba coherents, pot seleccionar la petició, marcant el checkbox de selecció, i prémer el botó **"Desactivar"**. D'aquesta forma, el compte d'usuari deixarà de ser vigent, i no tindrà funcionalitat a l'aplicació fins que no sigui reactivat de nou pel mateix administrador.

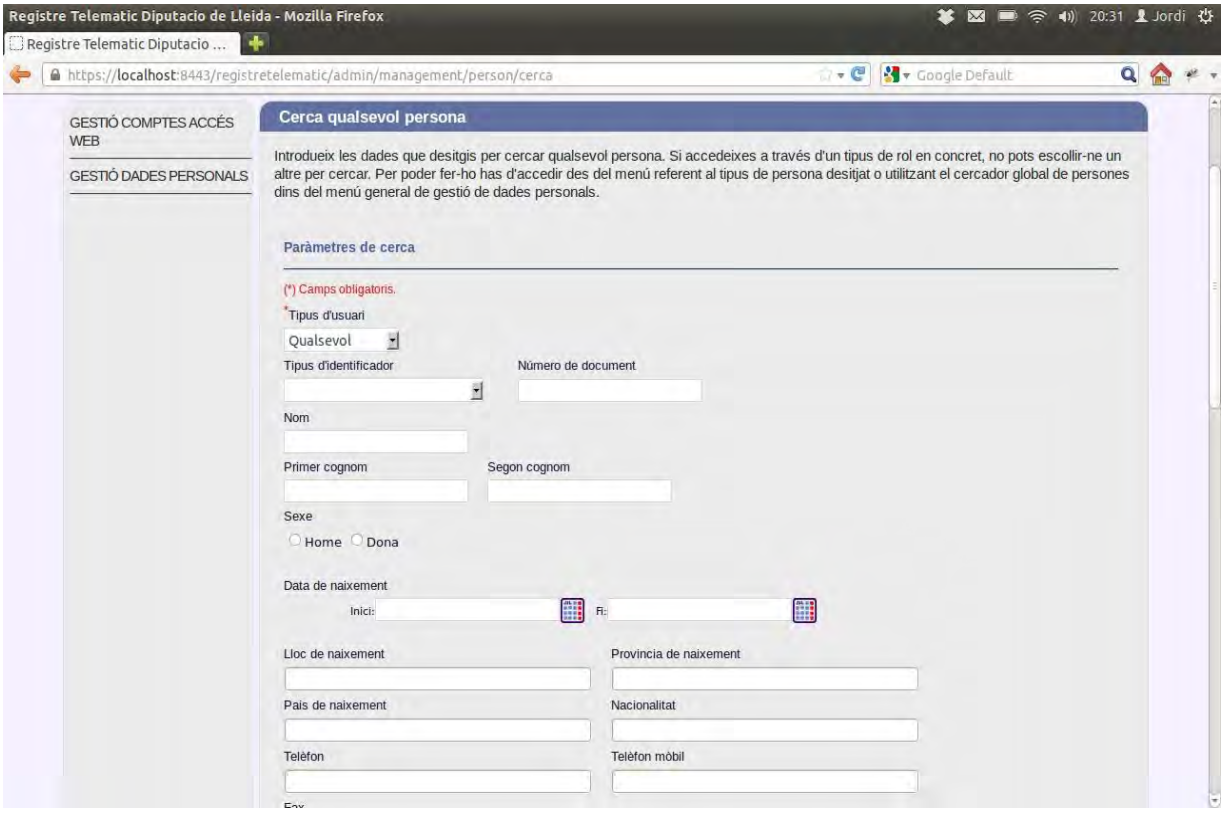
5.4.3 Gestió de dades personals

Aquesta segona entrada del menú principal permetrà a l'administrador consultar les dades personals dels diferents usuaris presents a l'aplicació. Qualsevol dels botons d'aquest submenú, adreçarà l'administrador a una cerca de persones. Per aquest motiu comentarem, en primer lloc, l'últim dels botons continguts en aquesta branca del menú, el **"Cercar persones"**, ja que la cerca d'usuaris d'un tipus determinat ("usuari", "empleat" o "administrador") serà la mateixa, però impedint modificar el tipus d'usuari.

És important matisar que, donat que entre les tasques de l'administrador no es troba el manteniment de les dades personals dels usuaris, només podrà realitzar consultes de les dades, que facilitaran la seva tasca de validació de altes, bloquejos o desactivacions de comptes web.

5.4.3.1 Cercar persones

Com s'acaba de comentar, el primer botó que tractarem en aquest apartat és el que està etiquetat com a **"Cercar persones"**. Aquest cercador ens permetrà buscar les persones emmagatzemades a la base de dades de l'aplicació (Il·lustració 173) permetent realitzar una cerca de persones, filtrant els resultats per tots els paràmetres que es troben en pantalla, i mostrant els resultats a la taula de la part inferior:



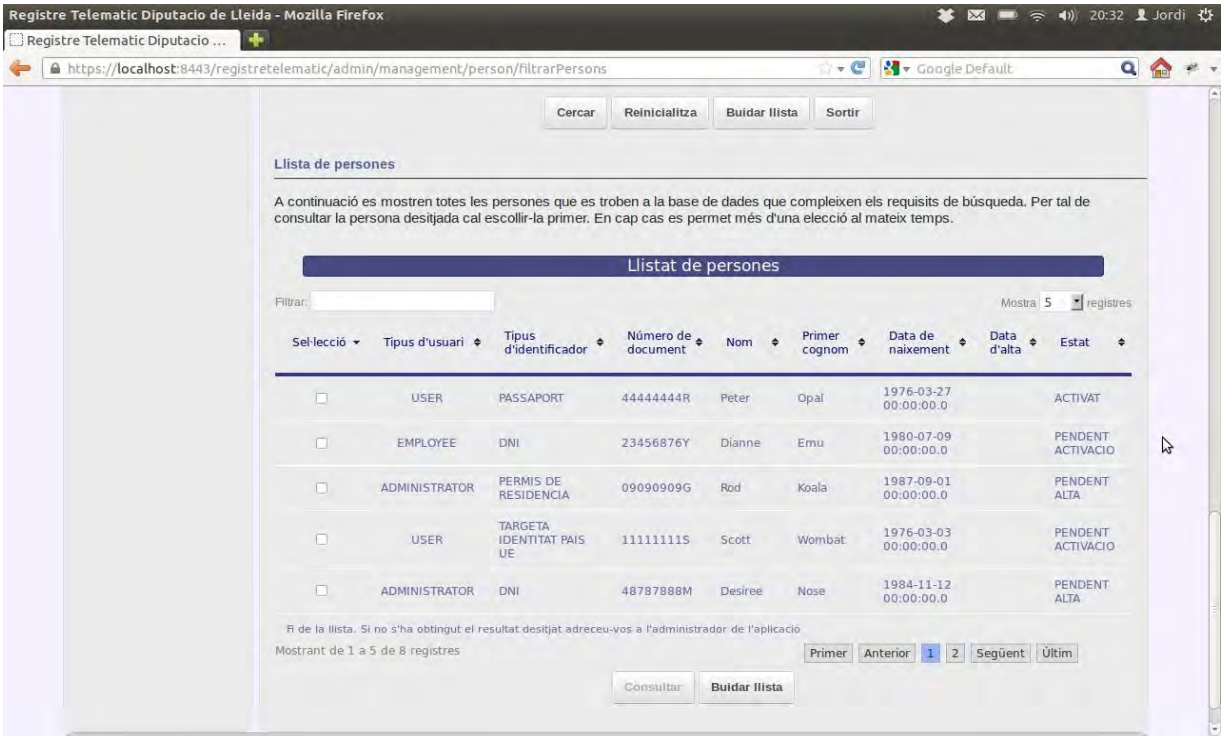
Il·lustració 173: Cercador d'usuaris global

- **Tipus d'usuari**: permet seleccionar el tipus d'usuari que volem buscar. Els possibles valors són "Administrador", "Empleat" o "Usuari". Existeix la possibilitat de cerca entre tots els tipus d'usuari marcant la opció **"Qualsevol"**.

- **Tipus d'identificador/Número de document**: permet triar el tipus de document mitjançant el qual la persona es va identificar per donar-se d'alta a l'aplicació, i el número d'aquest document.
- **Nom i cognoms**: permet cercar segons el nom i cognoms de l'usuari. La cerca es realitza per comparació de cadenes de text, de tal manera que, si només coneixem una part del nom, podem escriure només aquella part, i l'aplicació cercarà els usuaris que continguin aquella part.
- **Sexe**: segons si és home o dona. Si no es marca un dels dos, aquest paràmetre no es tindrà en compte (es mostraran els usuaris d'ambdós sexes).
- **Data de naixement**: l'aplicació permet acotar la data de naixement a dos dates concretes. Si no s'emplenen aquests camps, el paràmetre no es tindrà en compte. Si només es plena la data d'inicial, es mostraran les persones amb data de naixement posterior a la introduïda. Si només es plena la data final, es mostraran les persones amb data de naixement anterior a la introduïda.
- **Lloc de naixement**: permet buscar persones nascudes a una localitat concreta.
- **Província de naixement**: permet buscar persones nascudes a una província concreta.
- **País de naixement**: permet buscar persones nascudes a un país concret.
- **Nacionalitat**: permet buscar persones d'una nacionalitat concreta.
- **Telèfon**: permet buscar persones segons el seu telèfon.
- **Telèfon mòbil**: permet buscar persones segons el seu telèfon mòbil.
- **Fax**: permet buscar persones segons el seu fax.
- **Clau d'accés web**: permet cercar segons la seva contrasenya.
- **Estat**: permet cercar segons l'estat del compte a la base de dades.
- **Dates d'alta, baixa i modificació**: Aquestes dates corresponen als moments en que els registres de les persones que es troben a la base de dades han estat introduïts, modificats per darrera vegada, i donats de baixa, si és el cas. Si només es plena la data d'inicial, es mostraran les persones amb data d'alta, baixa o modificació posterior a la introduïda. Si només es plena la data final, es mostraran les persones amb data d'alta, baixa i modificació anterior a la introduïda.

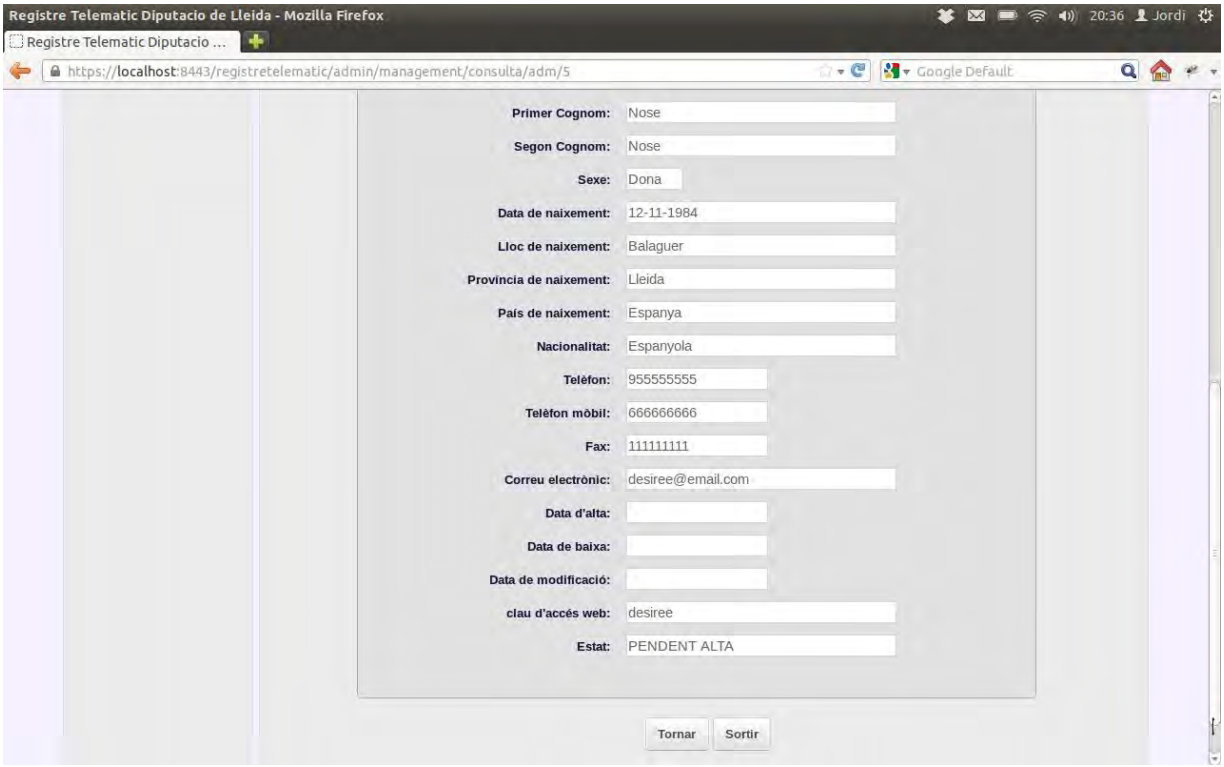
És possible també realitzar una ordenació dels resultats segons qualsevol dels paràmetres presents al desplegable “Ordenat per:”, i disposar-los de manera ascendent o descendent. Per realitzar la cerca, s'ha de prémer el botó **“Cercar”**. El botó **“Reinicialitza”** restaura tots els camps del cercador al seu estat per defecte. El botó **“Buidar llista”** permet buidar la llista de la taula inferior, corresponent a la darrera cerca realitzada. El botó **“Sortir”** ens porta directament a la pantalla inicial de l'aplicació.

La llista de la part inferior de la pantalla contindrà, com s'ha esmentat anteriorment, els resultats de la la darrera cerca realitzada (Il·lustració 174).



Il·lustració 174: Llistat de resultats de la cerca d'usuaris

Un cop la taula contingui resultats, l'administrador pot marcar qualsevol dels usuaris, i un cop fet, prémer el botó **"Consultar"** (Il·lustració 174), acció que ens portarà directament al formulari de consulta (Il·lustració 175) mostrant en pantalla les dades referents a l'usuari seleccionat. En aquesta pantalla podem sortir de la pàgina inicial prement el botó **"Sortir"**, o bé retornar al cercador de persones prement **"Tornar"**.

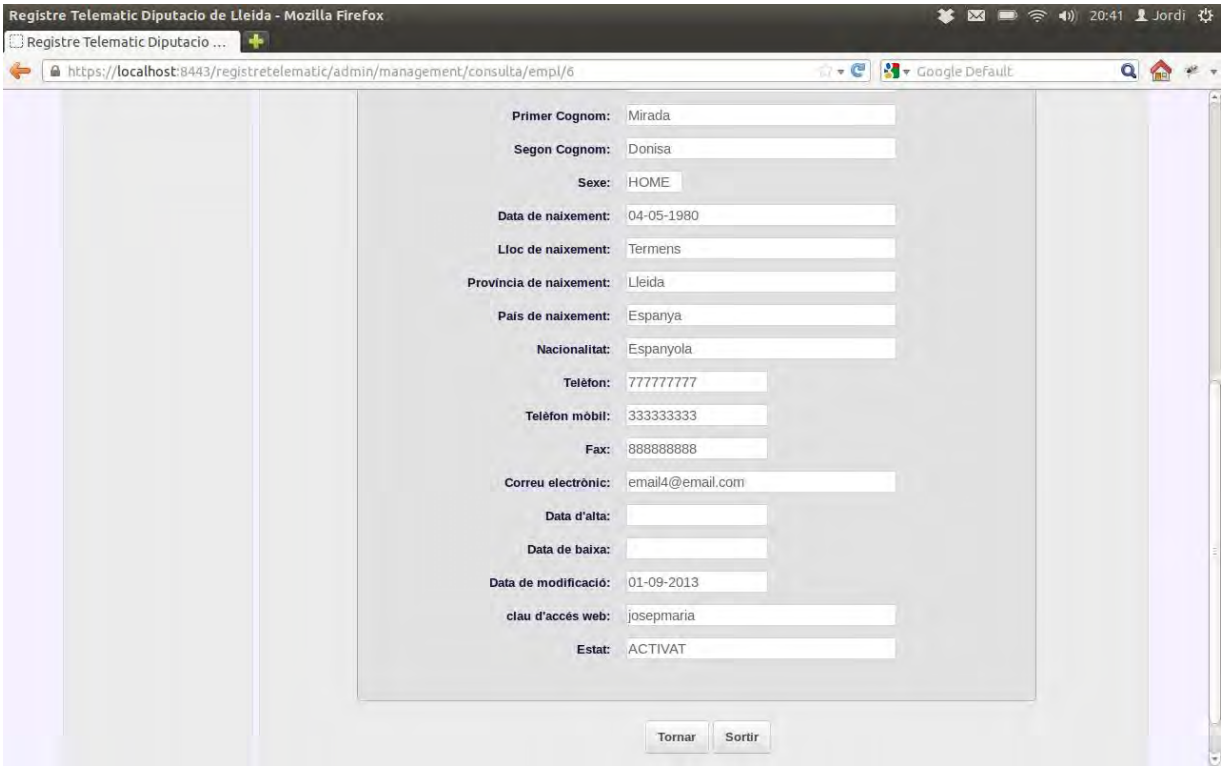


Il·lustració 175: Consulta d'usuari

5.4.3.2 Consulta d'usuaris

Els botons de **“Consulta”** portaran l'administrador directament al cercador de persones (5.4.3.1 Cercar persones). La única diferència amb el cercador de persones global, prèviament comentat, serà que el camp “Tipus d'usuari” apareixerà deshabilitat, i contindrà el tipus d'usuari que s'ha escollit per consultar, “Administrador”, “Empleat” o “Usuari”.

Per realitzar la cerca, l'administrador ha de completar els diferents camps que acotaran els resultats. Un cop premi el botó **“Cercar”**, els resultats seran mostrats a la taula inferior. Per realitzar la consulta, l'administrador ha de seleccionar un dels usuaris llistats, i prémer el botó inferior **“Consultar”**. Una nova finestra apareixerà en pantalla mostrant les dades corresponents a l'usuari marcat (Il·lustració 176).



Il·lustració 176: Consulta d'un empleat per part de l'administrador

Les dades d'aquest formulari no poden ser alterades, només consultades, donat que les tasques de l'administrador només són de validació de canvis als comptes web. A la part inferior d'aquesta pantalla trobem dos botons. **“Sortir”** ens portarà directament a la pantalla inicial de l'aplicació. **“Tornar”** ens retornarà al cercador de persones, mantenint les opcions de la darrera cerca realitzada.

6 Conclusions

Després de la realització del projecte “Registre Telemàtic”, les conclusions a les que hem arribat són les següents:

- S'han implementat amb èxit les diverses funcionalitats de l'aplicatiu web que permeten a l'Administració Pública interaccionar telemàticament amb els ciutadans.
- Gràcies a la utilització del “Registre Telemàtic”, s'aconsegueix una optimització dels recursos de l'Administració Pública, reduint el temps necessari per realitzar els seus tràmits habituals.
- La implementació de la signatura digital compleix les polítiques de seguretat estàndard per a les comunicacions telemàtiques emprant el DNI-e.
- L'ús dels certificats de signatura i d'autenticació del DNIe suposen una generalització d'aquests serveis de seguretat de cara a l'Administració Pública, donada la obligatorietat de tota la ciutadania de disposar d'aquest document acreditatiu per a la seva identificació.
- El fet que el “Registre Telemàtic” sigui una aplicació web i s'empri Java per a la signatura digital, fa que aquesta sigui accessible per a tots els usuaris independentment de la plataforma utilitzada.
- L'ús de tecnologies en constant evolució ha suposat l'adaptació de l'aplicació al llarg del seu desenvolupament. Això suposa un gran esforç a l'hora de conjuntar totes aquestes tecnologies en les seves diferents versions, i que aquestes interactuïn entre elles de forma fluida, per a assolir els objectius.
- La utilització únicament de software lliure en el desenvolupament de l'aplicació, ha resultat un gran benefici a nivell de programació, donat el cost zero de les eines emprades.

7 Treballs futurs

La creació de l'aplicació “Registre Telemàtic” ha estat un procés llarg i enriquidor. Però existeixen moltes funcionalitats que podrien ser afegides amb posterioritat, i que no han estat incloses en aquesta primera versió. En aquest apartat farem un breu resum del possibles treballs que podrien ser duts a terme a l'aplicació “Registre telemàtic”, per tal d'afegir funcionalitats interessants o nous mòduls per a realitzar altres tasques que pugui requerir una Administració Pública:

- Afegir mecanisme per recordar usuari i contrasenya durant un cert període de temps.
- Afegir un tercer tipus d'accés lliure per poder oferir accés a usuaris no registrats que necessitin algun tipus d'informació.
- Informar a l'usuari dels requisits i tecnologies que l'aplicació web requereix per al seu correcte funcionament.
- Actualitzar l'accés mitjançant el certificat d'autenticació del DNIe per a que ara sigui el propi Spring (Spring Security) qui gestioni l'obtenció del certificat i el login a l'aplicació. Possible implementació d'un LDAP que doni suport a aquest tipus d'autenticació.
- Implementar un mòdul per enviar correu electrònic automàticament informant dels estats en que es troben les diferents gestions dels usuaris. Això implica la implementació addicional d'un sistema de validació de comptes de correu electrònic al donar-se d'alta a l'aplicació.

  A més, agregar-hi un sistema de plantilles per la difusió de correus electrònics automatitzats.
- Agregar validació instantània dels comptes bancaris introduïts. Possiblement amb serveis web i Ajax.
- Implementar un sistema de control de data i hora extern al servidor utilitzant una autoritat de segellat de temps (TSA). Això permetria afegir valor legal a les dates de l'aplicació.
- Implementar altres tipus de signatura digital, entre elles les que afegeixen la data de creació. S'utilitzaria la TSA per afegir-hi la data certificada i tenir validesa davant un tribunal.
- Implementar algun sistema de log per a l'applet del DNI-e.
- Ampliar les funcionalitats de l'aplicació afegint la possibilitat de realitzar una signatura digital de prova per verificar el correcte funcionament del sistema.
- Ampliar els tràmits disponibles afegint-hi tràmits off-line. Aquests es troben en format pdf editables per omplir-hi les dades.
- Dotar a l'aplicació la funcionalitat de poder firmar pdfs i pujar-los posteriorment a la base de dades.
- Millorar sistema d'excepcions i informe de possibles errades tant de l'aplicació web com de l'applet del DNI-e.

Existirien moltes altres possibilitats, però aquí hem fet un recull de les que considerem importants a curt o mig termini.

8 Bibliografia

- Craig Walls. (2011). Spring Tercera Edición. Anaya Multimedia.
- Craig Walls with Ryan Breindenbach. (2007). Spring in Action Second Edition. Greenwich: Manning
- Thomas Van de Velde, Bruce Snyder, Christian Dupuis, Sing Li, Anne Horton, and Naveen Balani . (2007). Beginning Spring Framework 2 . Indianapolis:Wiley Publishing, Inc.
- Peter Mularien. (2010). Spring Security 3. Birmingham: Packt Publishing Ltd.
- Ira R. Forman, Nate Forman. (2004). Java Reflection in Action. Manning.
- Herbert Schildt. (2005). La biblia de java 2 v5.0. Madrid: Anaya Multimedia.

- http://www.springsource.org/spring-framework
- http://www.springsource.org/spring-security
- http://static.springsource.org/spring/docs/3.0.x/spring-framework-reference/html/
- http://static.springsource.org/spring/docs/3.1.x/spring-framework-reference/html/
- http://static.springsource.org/spring/docs/3.2.x/spring-framework-reference/html/
- http://static.springsource.org/spring-security/site/docs/3.1.x/reference/springsecurity.html
- http://www.springhispano.org/
- http://forum.springsource.org/
- http://www.mkyong.com/tutorials/spring-mvc-tutorials/
- http://www.mkyong.com/tutorials/spring-security-tutorials/
- http://www.mkyong.com/tutorials/hibernate-tutorials/
- http://viralpatel.net/blogs/tutorial-save-get-blob-object-spring-3-mvc-hibernate/
- http://levelup.lishman.com/
- http://www.java-forums.org/blogs/spring-framework/
- http://www.adictosaltrabajo.com/
- http://stackoverflow.com/
- http://docs.oracle.com/
- http://www.dnielectronico.es/
- http://zonatic.usatudni.es/
- http://www.codestore.net/store.nsf/unid/DOMM-4UTFCP
- http://www.developer.com/java/other/article.php/3587361/Java-Applet-for-Signing-with-a-Smart-Card.htm

- http://ludovic.rousseau.free.fr/softwares/pcsc-tools/
- http://www.bouncycastle.org/java.html
- http://www.kriptopolis.org/
- http://infow.wordpress.com/2009/01/11/openssl-la-navaja-suiza-del-cifrado/
- http://docs.oracle.com/javase/7/docs/technotes/guides/plugin/developer_guide/rsa_signing.html
- http://www.adictosaltrabajo.com/tutoriales/tutoriales.php?pagina=app_keyt_jars
- http://tomcat.apache.org/
- http://tiles.apache.org/
- http://mvnrepository.com/
- http://www.w3schools.com/
- http://jqueryui.com/dialog/
- https://datatables.net/
- http://www.govannom.org/index.php/seguridad/7-criptografia/439-historia-de-la-criptografia
- http://es.wikipedia.org/
- http://www.genbetadev.com/seguridad-informatica/que-es-y-como-surge-la-criptografia-un-repaso-por-su-historia
- http://redyseguridad.fi-p.unam.mx/proyectos/criptografia/criptografia/index.php/1-panorama-general/12-historia-de-la-criptografia?showall=&start=3
- http://histinf.blogs.upv.es/2010/11/01/breve-biografia-de-alan-turing/
- http://www.textoscientificos.com/criptografia/hill
- http://alt1040.com/2011/07/la-maquina-enigma-el-sistema-de-cifrado-que-puso-en-jaque-a-europa
- http://bolsaydatos.com/claude-e-shannon-el-sabio-malabarista.html
- http://claudeelwoodshannon.blogspot.com.es/
- http://www.javiercampos.es/blog/2011/07/22/el-algoritmo-de-diffie-hellman/
- http://www.arielorellana.net/des.htm
- http://personal.telefonica.terra.es/web/jms32/Cifra/CodSecretos/Cap06/Cap0610.html
- http://personal.telefonica.terra.es/web/jms32/Cifra/CodSecretos/Cap06/Cap0603.html#LaCifraDES
- http://www.ecured.cu/index.php/ElGamal
- http://www.slideshare.net/GAlbertoHoyos/cifrado-elgamal
- www.giac.org/cissp-papers/42.pdf
- http://orlingrabbe.com/des.htm

- http://seguinfo.wordpress.com/2007/10/02/%C2%BFque-es-la-criptografia-de-curva-eliptica/
- www.hezkuntza.ejgv.euskadi.net
- www.itescam.mx-edu
- http://www.certsuperior.com/FirmasDigitales.aspx
- https://www.cgcom.es/que_es
- http://www.boe.es/buscar/doc.php?id=BOE-A-2003-23399
- http://www.upv.es/contenidos/CD/info/711250normalc.html
- http://gaussianos.com/algoritmos-hash-i-introduccion/
- www.boe.es/boe_catalan/dias/2004/01/01/pdfs/A00137-00151.pdf
- http://www.smartcardbasics.com/smart-card-overview.html
- http://www.kriptopolis.org/opendnie-listo
- http://robertoluis.wordpress.com/2011/12/13/que-es-un-orm-y-por-que-nos-interesa/
- http://www.programacion.com/articulo/tomcat_-_introduccion_134
- www.abaco.edu.pe/Manuales%5CLenguaje%20de%20programaci%C3%B3n%20Java%5CEl%20lenguaje%20de%20programaci%C3%B3n%20Java%20NXT.pdf
- http://mundogeek.net/archivos/2004/10/04/una-no-tan-breve-historia-de-java/
- http://jcesarperez.blogspot.com.es/2009/03/por-que-maven.html
- http://aprenderinternet.about.com/od/Glosario/g/Applet-En-Java.htm
- http://www.alegsa.com.ar/Dic/applet.php
- http://j2ee.ibsi.cl/desarrollo/java-j2ee/tecnologia-jsp-java-server-pages/
- http://www.lab.inf.uc3m.es/~a0080802/RAI/servlet.html

Apèndixs

Apèndix Llei 59/2003 sobre el DNI-electrònic

Butlletí oficial de l'estat

ANY CCCXLIV

DIJOUS 1 DE GENER DE 2004

SUPLEMENT NÚM. 1 EN LLENGUA CATALANA

FASCICLE SEGON

CAP DE L'ESTAT

23399 LLEI 59/2003, de 19 de desembre, de signatura electrònica. («BOE» 304, de 20-12-2003.)

JUAN CARLOS I

REI D'ESPANYA

A tots els qui vegeu i entengueu aquesta Llei.

Sapigueu: Que les Corts Generals han aprovat la Llei següent i jo la sanciono.

EXPOSICIÓ DE MOTIUS

I

El Reial decret llei 14/1999, de 17 de setembre, sobre signatura electrònica, va ser aprovat amb l'objectiu de fomentar la ràpida incorporació de les noves tecnologies de seguretat de les comunicacions electròniques en l'activitat de les empreses, els ciutadans i les administracions públiques. D'aquesta manera, es coadjuvava a potenciar el creixement i la competitivitat de l'eco-

nomia espanyola mitjançant l'establiment ràpid d'un marc jurídic per a la utilització d'una eina que aporta confiança en la realització de transaccions electròniques en xarxes obertes com és el cas d'Internet. El Reial decret llei esmentat va incorporar a l'ordenament públic espanyol la Directiva 1999/93/CE del Parlament Europeu i del Consell, de 13 de desembre de 1999, per la qual

s'estableix un marc comunitari per a la signatura electrònica, fins i tot abans de la seva promulgació i publicació al «Diari Oficial de les Comunitats Europees».

Després de la seva ratificació pel Congrés dels Diputats, es va acordar la tramitació del Reial decret

llei 14/1999 com a projecte de llei, a fi de sotmetre'l a una consulta pública més àmplia i al debat parlamentari posterior per perfeccionar-ne el text. Això no obstant, aquesta iniciativa va decaure en

expirar el mandat de les cambres el març de 2000. Aquesta Llei, per tant, és el resultat del compromís assumit en la VI Legislatura, i actualitza alhora el marc establert al Reial decret llei

14/1999 mitjançant la incorporació de les modificacions que aconsella l'experiència acumulada des de la seva entrada en vigor tant al nostre país com en l'àmbit internacional.

II

El desenvolupament de la societat de la informació i la difusió dels efectes positius que en deriven exigeix a generalització de la confiança dels ciutadans en les comunicacions telemàtiques. Amb tot, les dades més recents assenyalen que encara hi ha desconfiança per part dels que intervenen en les transaccions telemàtiques i, en general, en les comunicacions que les noves tecnologies permeten a l'hora de transmetre informació, manca de confiança que constitueix un fre per al desenvolupament de la societat de la informació, en particular, l'Administració i el comerç electrònics.

Com a resposta a aquesta necessitat de conferir seguretat a les comunicacions per Internet sorgeix, entre altres, la signatura electrònica. La signatura electrònica constitueix un instrument capaç de permetre una comprovació de la procedència i de la integritat dels missatges intercanviats a través de xarxes de telecomunicacions, que ofereix les bases per evitar el rebuig, si s'adopten les mesures oportunes basant-se en dates electròniques.

Els subjectes que fan possible l'ús de la signatura electrònica són els denominats prestadors de serveis de certificació. Per a això expedeixen certificats electrònics, que són documents electrònics que relacionen les eines de signatura electrònica en poder de cada usuari amb la seva identitat personal, i d'aquesta manera el donen a conèixer en l'àmbit telemàtic com a signant.

La llei obliga els prestadors de serveis de certificació a efectuar una tutela i gestió permanent dels certificats electrònics que expedeixen. Els detalls d'aquesta gestió s'han de recollir en l'anomenada declaració de pràctiques de certificació, on s'especifiquen les condicions aplicables a la so icitud, l'expedició, l'ús, la suspensió i l'extinció de la vigència dels certificats electrònics. A més, aquests prestadors estan obligats a mantenir accessible un servei de consulta sobre l'estat de vigència dels certificats en què s'ha d'indicar de manera actualitzada si aquests estan vigents o si la seva vigència ha estat suspesa o extingida.

Així mateix, s'ha de destacar que la Llei defineix una classe particular de certificats electrònics denominats certificats reconeguts, que són els certificats electrònics que s'han expedit complint requisits qualificats pel que fa al contingut, als procediments de comprovació de la identitat del signant i a la fiabilitat i les garanties de l'activitat de certificació electrònica.

Els certificats reconeguts constitueixen una peça fonamental de l'anomenada signatura electrònica reconeguda, que es defineix seguint les pautes que imposa la Directiva 1999/93/CE com la signatura electrònica avançada basada en un certificat reconegut i generada mitjançant un dispositiu segur de creació de signatura. La llei atorga a la signatura electrònica reconeguda l'equivalència funcional amb la signatura manuscrita respecte de les dades consignades en forma electrònica.

D'altra banda, la Llei conté les garanties que han de complir els dispositius de creació de signatura perquè puguin ser considerats dispositius segurs i conformar així una signatura electrònica reconeguda.

La certificació tècnica dels dispositius segurs de creació de signatura electrònica es basa en el

marc que estableixen la Llei 21/1992, de 16 de juliol, d'indústria, i les seves disposicions de desplegament. Per a aquesta certificació s'utilitzen les normes tècniques publicades a aquests efectes en el «Diari Oficial de les Comunitats Europees» o, excepcionalment, les aprovades pel Ministeri de Ciència i Tecnologia.

Addicionalment, la Llei estableix un marc d'obligacions aplicables als prestadors de serveis de certificació, en funció de si aquests emeten certificats reconeguts o no, i determina el seu règim de responsabilitat, tenint en compte els deures de diligència que incumbeixen als signants i als tercers destinataris de documents signats electrònicament.

III

Aquesta Llei es promulga per reforçar el marc jurídic existent i s'incorporen al seu text algunes novetats respecte del Reial decret llei 14/1999 que contribuiran a dinamitzar el mercat de la prestació de serveis de certificació.

Així, es revisa la terminologia, es modifica la sistemàtica i se simplifica el text per facilitar-ne la comprensió i dotar-lo d'una estructura més concorde amb la nostra tècnica legislativa.

Una de les novetats que la Llei ofereix respecte del Reial decret llei 14/1999 és la denominació com a signatura electrònica reconeguda de la signatura electrònica que s'equipara funcionalment a la signatura manuscrita.

Es tracta simplement de la creació d'un concepte nou demanat pel sector, sense que això impliqui cap modificació dels requisits substantius que tant la Directiva 1999/93/CE com el mateix Reial decret llei 14/1999 exigien. Amb això s'aclareix que no n'hi ha prou amb la signatura electrònica avançada per a l'equiparació amb la signatura manuscrita; cal que la signatura electrònica avançada

estigui basada en un certificat reconegut i hagi estat creada per un dispositiu segur de creació.

Així mateix, s'ha de destacar de manera particular l'eliminació del registre de prestadors de serveis de certificació, que ha donat pas a l'establiment d'un mer servei de difusió d'informació sobre els prestadors que operen al mercat, les certificacions de qualitat i les característiques dels productes i serveis de què disposen per dur a terme la seva activitat.

D'altra banda, la Llei modifica el concepte de certificació de prestadors de serveis de certificació per atorgar-li un grau de llibertat més gran i donar més protagonisme a la participació del sector privat en els sistemes de certificació i eliminant les presumpcions legals que hi estan associades, per adaptar-se de manera més precisa al que estableix la Directiva. Així, s'afavoreix l'autoregulació de la indústria, de manera que sigui aquesta qui dissenyi i gestioni, d'acord amb les seves pròpies necessitats, sistemes voluntaris d'acreditació destinats a millorar els nivells tècnics i de qualitat en la prestació de serveis de certificació. El nou règim neix des del convenciment que els segells de qualitat són un instrument eficaç per convèncer els usuaris dels avantatges dels productes i serveis de certificació electrònica, i que és imprescindible facilitar i agilitar l'obtenció d'aquests símbols externs per als qui els ofereixen al públic. Si bé es recullen fidelment en la Llei els conceptes d'«acreditació» de prestadors de serveis de certificació i de «conformitat» dels dispositius segurs de creació de signatura electrònica que conté la Directiva, la terminologia s'ha adaptat a la més comunament emprada i coneguda recollida a la Llei 21/1992, de 16 de juliol, d'indústria.

Una altra modificació rellevant és que la Llei clarifica l'obligació de constitució d'una garantia econòmica per part dels prestadors de serveis de certificació que emetin

certificats reconeguts, i estableix una quantia mínima única de tres milions d'euros i, a més,

flexibilitza la combinació dels diferents instruments per constituir la garantia.

D'altra banda, ja que la prestació de serveis de certificació no està subjecta a autorització prèvia, és important destacar que la Llei reforça les capacitats d'inspecció i control del Ministeri de Ciència i Tecnologia, ja que assenyala que aquest departament pot ser assistit d'entitats independents i tècnicament qualificades per efectuar les tasques de supervisió i control sobre els prestadors de serveis de certificació.

També s'ha de destacar la regulació que la Llei conté respecte del document nacional d'identitat electrònic, que s'erigeix en un certificat electrònic reconegut cridat a generalitzar l'ús d'instruments segurs de comunicació electrònica capaços de conferir la mateixa integritat i autenticitat que la que actualment envolta les comunicacions a través de mitjans físics. La Llei es limita a fixar el marc normatiu bàsic del nou DNI electrònic i posa de manifest les seves dues notes més característiques —acredita la identitat del titular en qualsevol procediment administratiu i permet la signatura electrònica de documents—, i es remet a la normativa específica quant a les particularitats del seu règim jurídic.

Així mateix, una altra novetat és l'establiment en la Llei del règim aplicable a l'actuació de persones jurídiques com a signants, a l'efecte d'integrar aquestes entitats al tràfic telemàtic. Així es va més enllà del Reial decret llei de 1999, que només permetia a les persones jurídiques ser titulars de certificats electrònics en l'àmbit de la gestió dels tributs. Precisament, l'enorme expansió que han tingut aquests certificats en l'esmentat àmbit els últims anys, sense que això hagi representat cap augment de la litigiositat ni d'inseguretat jurídica en les transaccions, aconsellen la generalització de la titularitat de certificats per persones morals.

En tot cas, els certificats electrònics de persones jurídiques no alteren la legislació civil i mercantil quant a la figura del representant orgànic o voluntari i no substitueixen els certificats electrònics que s'expedeixin a persones físiques en què es reflecteixin aquestes relacions de representació.

Com a ressorts de seguretat jurídica, la Llei exigeix, d'una banda, una legitimació especial perquè les persones físiques sol·licitin l'expedició de certificats; d'altra banda, obliga els sol·licitants a responsabilitzar-se de la custòdia de les dades de creació de signatura electrònica associades a aquests certificats, tot això sense perjudici que puguin ser utilitzats per altres persones físiques vinculades a l'entitat. Finalment, pel que fa a tercers, limita l'ús d'aquests certificats als actes que integrin la relació entre la persona jurídica i les administracions públiques i a les coses o serveis que constitueixen el gir o tràfic ordinari de l'entitat, sense perjudici dels possibles límits quantitatius o qualitatius que s'hi puguin afegir. Es tracta de conjugar el dinamisme que ha de presidir l'ús d'a-

quests certificats en el tràfic amb les necessàries dosis de prudència i seguretat per evitar que puguin néixer obligacions incontrolables davant tercers a causa d'un ús inadequat de les dades de creació de signatura. L'equilibri entre un principi i l'altre s'ha establert sobre les coses i els serveis que constitueixen el gir o tràfic ordinari de l'empresa de manera para ela a com el nostre més que centenari Codi de comerç regula la vinculació davant tercers dels actes de comerç realitzats pel factor de l'establiment.

Amb l'expressió «gir o tràfic ordinari» d'una entitat s'actualitza a un vocabulari més concorde amb els nostres dies el que en la legislació mercantil espanyola es denomina «establiment fabril o mercantil». Amb això es comprenen les transaccions efectuades mediatament o immediatament per a la realització del nucli d'activitat de l'entitat i les activitats de gestió o administratives necessàries per exercir-la, com ara la contractació de subministraments tangibles i intangibles o de serveis auxiliars. Finalment, s'ha de recalcar que, encara que el «gir o tràfic ordinari» sigui un terme encunyat pel dret mercantil, la regulació sobre els certificats de persones jurídiques no només

s'aplica a les societats mercantils, sinó a qualsevol tipus de persona jurídica que vulgui fer ús de la signatura electrònica en la seva activitat.

Addicionalment, s'afegeix un règim especial per a l'expedició de certificats electrònics a entitats sense personalitat jurídica a què es refereix l'article 33 de la Llei general tributària, únicament a l'efecte de la seva utilització en l'àmbit tributari, en els termes que estableixi el Ministeri d'Hisenda.

D'altra banda, seguint la pauta marcada per la Llei 34/2002, d'11 de juliol, de serveis de la societat de la informació i de comerç electrònic, s'inclou dins de la modalitat de prova documental el suport en el qual consten les dades signades electrònicament, que dóna més seguretat jurídica a l'ús de la signatura electrònica en sotmetre-la a les regles d'eficàcia en judici de la prova documental.

A més, s'ha de destacar que un altre aspecte nou de la Llei és l'acolliment explícit que s'efectua de les relacions de representació subjacents que poden existir en l'ús de la signatura electrònica. No hi ha dubte que l'institut de la representació està àmpliament generalitzat en el tràfic econòmic, d'aquí la conveniència de dotar de seguretat jurídica la imputació a l'esfera jurídica del representat en les declaracions que cursa el representant a través de la signatura electrònica. Per a això, s'estableix

com a novetat que en l'expedició de certificats reconeguts que admetin entre els seus atributs relacions de representació, aquesta ha d'estar emparada en un document públic que acrediti fefaentment l'esmentada relació de representació així com la suficiència i la idoneïtat dels poders conferits al representant. Així mateix, es preveuen mecanismes per assegurar el manteniment de

les facultats de representació durant tota la vigència del certificat reconegut.

Finalment, s'ha de destacar que la Llei permet que els prestadors de serveis de certificació, amb l'objectiu de millorar la confiança en els seus serveis, poden establir mecanismes de coordinació amb les dades que preceptivament hagin de constar als registres públics, en particular, mitjançant connexions telemàtiques, a l'efecte de verificar les dades que figuren als certificats en el moment d'expedir-los. Aquests mecanismes de coordinació també poden preveure la notificació telemàtica

per part dels registres als prestadors de serveis de certificació de les variacions registrals posteriors.

IV

La Llei consta de 36 articles agrupats en sis títols, 10 disposicions addicionals, dues disposicions transitòries, una disposició derogatòria i tres disposicions finals.

El títol I conté els principis generals que delimiten els àmbits subjectiu i objectiu d'aplicació de la Llei, els efectes de la signatura electrònica i el règim d'ús davant les administracions públiques i d'accés a l'activitat de prestació de serveis de certificació.

El règim aplicable als certificats electrònics consta al títol II, que dedica el primer capítol a determinar qui poden ser els seus titulars i a regular les vicissituds que afecten la seva vigència. El capítol II regula els certificats reconeguts, i el tercer, el document nacional d'identitat electrònic.

El títol III regula l'activitat de prestació de serveis de certificació i estableix les obligacions a què estan subjectes els prestadors —distingint amb nitidesa les que només afecten els que expedeixen certificats reconeguts—, i el règim de responsabilitat aplicable.

El títol IV estableix els requisits que han de complir els dispositius de verificació i creació de signatura electrònica i el procediment que s'ha de seguir per obtenir segells de qualitat en l'activitat de prestació de serveis de certificació.

Els títols V i VI dediquen el seu contingut, respectivament, a fixar els règims de supervisió i sanció dels prestadors de serveis de certificació.

Finalment, tanquen el text les disposicions addicionals —que al·ludeixen als règims especials que són d'aplicació preferent—, les disposicions transitòries —que incorporen seguretat jurídica a l'activitat desplegada a l'empara de la normativa anterior—, la disposició derogatòria i les disposicions finals relatives al fonament constitucional, l'habilitació per al desplegament reglamentari i l'entrada en vigor.

Aquesta disposició ha estat sotmesa al procediment d'informació en matèria de normes i reglamentacions tècniques que preveuen la Directiva 98/34/CE, del Parlament Europeu i del Consell, de 22 de juny de 1998, per la qual s'estableix un procediment d'informació en matèria de normes i reglamentacions tècniques, modificada per la Directiva 98/48/CE, del Parlament Europeu

i del Consell, de 20 de juliol de 1998, i el Reial decret 1337/1999, de 31 de juliol, pel qual es regula la tramesa d'informació en matèria de normes i reglamentacions tècniques i reglaments relatius als serveis de la societat de la informació.

TÍTOL I

Disposicions generals

Article 1. Objecte.

1. Aquesta Llei regula la signatura electrònica, la seva eficàcia jurídica i la prestació de serveis de certificació.

2. Les disposicions que conté aquesta Llei no alteren les normes relatives a la subscripció, la formalització, la validesa i l'eficàcia dels contractes i qualssevol altres actes jurídics ni les relatives als documents en què uns i altres constin.

Article 2. Prestadors de serveis de certificació subjectes a la Llei.

1. Aquesta Llei s'aplica als prestadors de serveis de certificació establerts a Espanya i als serveis de certificació que els prestadors residents o domiciliats en un altre Estat ofereixin a través d'un establiment permanent situat a Espanya.

2. Es denomina prestador de serveis de certificació la persona física o jurídica que expedeix certificats electrònics o presta altres serveis en relació amb la signatura electrònica.

3. S'entén que un prestador de serveis de certificació està establert a Espanya quan la seva residència o domicili social estigui en territori espanyol, sempre que aquests coincideixin amb el lloc on estigui efectivament centralitzada la gestió administrativa i la direcció dels seus negocis. Altrament, cal atenir-se al lloc on es dugui a terme la gestió o direcció esmentada.

4. Es considera que un prestador opera mitjançant un establiment permanent situat en territori espanyol quan hi tingui, de forma continuada o habitual, instal·lacions o llocs de treball en què dugui a terme tota o part de la seva activitat.

5. Es presumeix que un prestador de serveis de certificació està establert a Espanya quan l'esmentat prestador o alguna de les seves sucursals s'hagi inscrit al Registre Mercantil o en un altre registre públic espanyol en el qual sigui necessària la inscripció per adquirir personalitat jurídica.

La mera utilització de mitjans tecnològics situats a Espanya per a la prestació o l'accés al servei no implica, per si sola, l'establiment del prestador a Espanya.

Article 3. Signatura electrònica i documents signats electrònicament.

1. La signatura electrònica és el conjunt de dades en forma electrònica, consignades al costat d'altres o associades amb aquestes, que poden ser utilitzades com a mitjà d'identificació del signant.

2. La signatura electrònica avançada és la signatura electrònica que permet identificar el signant i detectar qualsevol canvi ulterior de les dades signades, que està vinculada al signant de manera única i a les dades a les quals es refereix i que ha estat creada per mitjans que el signant pot mantenir sota el seu control exclusiu.

3. Es considera signatura electrònica reconeguda la signatura electrònica avançada basada en un certificat reconegut i generada mitjançant un dispositiu segur de creació de signatura.

4. La signatura electrònica reconeguda té, respecte de les dades consignades en forma electrònica, el mateix valor que la signatura manuscrita en relació amb les dades consignades en paper.

5. Es considera document electrònic el redactat en suport electrònic que incorpori dades que estiguin signades electrònicament.

6. El document electrònic és suport de:

a) Documents públics, perquè estan signats electrònicament per funcionaris que tenen legalment atribuïda la facultat de donar fe pública, judicial, notarial o administrativa, sempre que actuïn en l'àmbit de les seves competències amb els requisits que exigeix la Llei en cada cas.

b) Documents expedits i signats electrònicament per funcionaris o empleats públics en l'exercici de les seves funcions públiques, d'acord amb la seva legislació específica.

c) Documents privats.

7. Els documents a què es refereix l'apartat anterior tenen el valor i l'eficàcia jurídica que correspon a la seva respectiva naturalesa, de conformitat amb la legislació que els és aplicable.

8. El suport en el qual estiguin les dades signades electrònicament és admissible com a prova documental en judici. Si s'impugna l'autenticitat de la signatura electrònica reconeguda, amb la qual s'hagin signat les dades incorporades al document electrònic, s'ha de comprovar que el prestador de serveis de certificació, que expedeix els certificats electrònics, compleix tots els requisits que estableix la Llei pel que fa a la garantia dels serveis que presta en la comprovació de l'eficàcia de la signatura electrònica, i en especial, les obligacions de garantir la confidencialitat del procés així com l'autenticitat, la conservació i la integritat de la informació generada i la identitat dels signants. Si s'impugna l'autenticitat de la signatura electrònica avançada, amb la qual s'hagin signat les dades incorporades al document electrònic, cal atenir-se al que estableix l'apartat 2 de l'article 326 de la Llei d'enjudiciament civil.

9. No s'han de negar efectes jurídics a una signatura electrònica que no compleixi els requisits de signatura electrònica reconeguda en relació amb les dades a les quals estigui associada pel mer fet de presentar-se en forma electrònica.

10. Als efectes del que disposa aquest article, quan una signatura electrònica s'utilitzi conformement a les condicions acordades per les parts per relacionar-se entre si, s'ha de tenir en compte el que aquestes hagin estipulat.

Article 4. Ús de la signatura electrònica en l'àmbit de les administracions públiques.

1. Aquesta Llei s'aplica a l'ús de la signatura electrònica al si de les administracions públiques, els seus organismes públics i les entitats que en depenen o que hi estan vinculades i en les relacions que mantinguin aquelles i aquests entre si o amb els particulars.

Les administracions públiques, per tal de salvaguardar les garanties de cada procediment, poden establir condicions addicionals a la utilització de la signatura electrònica en els procediments. Les condicions poden incloure, entre altres, la imposició de dates electròniques sobre els documents electrònics integrats a un expedient administratiu. S'entén per data electrònica el conjunt de

dades en forma electrònica utilitzades com a mitjà per constatar el moment en què s'ha efectuat una actuació sobre altres dades electròniques a les quals estan associades.

2. Les condicions addicionals a les quals es refereix l'apartat anterior només poden fer referència a les característiques específiques de l'aplicació de què es tracti i han de garantir el compliment del que preveu l'article 45 de la Llei 30/1992, de 26 de novembre, de règim jurídic de les administracions públiques i del procediment administratiu comú. Aquestes condicions han de ser

objectives, proporcionades, transparents i no discriminatòries i no han d'obstaculitzar la prestació de serveis de certificació al ciutadà quan hi intervinguin diferents administracions públiques nacionals o de l'Espai Econòmic Europeu.

3. Les normes que estableixin condicions generals addicionals per a l'ús de la signatura electrònica davant de l'Administració General de l'Estat, els seus organismes públics i les entitats que en depenen o que hi estan vinculades s'han de dictar a proposta conjunta dels ministeris d'Administracions Públiques i de Ciència i Tecnologia i amb l'informe previ del Consell Superior d'Informàtica i per a l'impuls de l'Administració Electrònica.

4. La utilització de la signatura electrònica en les comunicacions que afecten la informació classificada, la seguretat pública o la defensa nacional es regeix per la seva normativa específica.

Article 5. Règim de prestació dels serveis de certificació.

1. La prestació de serveis de certificació no està subjecta a autorització prèvia i es du a terme en règim de lliure competència. No es poden establir restriccions per als serveis de certificació que procedeixin d'un altre Estat membre de l'Espai Econòmic Europeu.

2. Els òrgans de defensa de la competència han de vetllar pel manteniment de condicions de competència efectiva en la prestació de serveis de certificació al públic mitjançant l'exercici de les funcions que tinguin legalment atribuïdes.

3. La prestació al públic de serveis de certificació per les administracions públiques, els seus organismes públics o les entitats que en depenen o que hi estan vinculades s'ha de dur a terme

d'acord amb els principis d'objectivitat, transparència i no-discriminació.

TÍTOL II

Certificats electrònics

CAPÍTOL I

Disposicions generals

Article 6. Concepte de certificat electrònic i de signant.

1. Un certificat electrònic és un document signat electrònicament per un prestador de serveis de certificació que vincula unes dades de verificació de signatura a un signant i confirma la seva identitat.

2. El signant és la persona que posseeix un dispositiu de creació de signatura i que actua en nom propi en nom d'una persona física o jurídica a la qual representa.

Article 7. Certificats electrònics de persones jurídiques.

1. Poden sol·licitar certificats electrònics de persones jurídiques els seus administradors, representants legals i voluntaris amb poder validat a aquests efectes.

Els certificats electrònics de persones jurídiques no poden afectar el règim de representació orgànica o voluntària que regula la legislació civil o mercantil aplicable a cada persona jurídica.

2. La custòdia de les dades de creació de signatura associades a cada certificat electrònic de persona jurídica és responsabilitat de la persona física sol·licitant, la identificació de la qual s'inclou al certificat electrònic.

3. Les dades de creació de signatura només poden ser utilitzades quan s'admeti en les relacions que mantingui la persona jurídica amb les administracions públiques o en la contractació de béns o serveis que siguin propis o concernents al seu gir o tràfic ordinari. Així mateix, la persona jurídica pot imposar límits addicionals, per raó de la quantia o de la matèria, per a l'ús de les dades esmentades que, en tot cas, han de figurar al certificat electrònic.

4. S'entenen fets per la persona jurídica els actes o contractes en què la seva signatura s'hagi emprat dins els límits que preveu l'apartat anterior. Si la signatura s'utilitza transgredint els límits esmentats, la persona jurídica queda vinculada davant tercers només si els assumeix com a propis o s'han fet en interès seu. En cas contrari, els efectes dels actes esmentats recauen sobre la persona física responsable de la custòdia de les dades de creació de signatura, que pot repetir, si s'escau, contra qui les hagi utilitzat.

5. El que disposa aquest article no és aplicable als certificats que serveixin per verificar la signatura electrònica del prestador de serveis de certificació amb què signi els certificats electrònics que expedeixi.

6. El que disposa aquest article no és aplicable als certificats que s'expedeixin a favor de les administracions públiques, que estan subjectes a la seva normativa específica.

Article 8. Extinció de la vigència dels certificats electrònics.

1. Són causes d'extinció de la vigència d'un certificat electrònic:

a) Expiració del període de validesa que figura al certificat.

b) Revocació formulada pel signant, la persona física o jurídica representada per aquest, un tercer autoritzat o la persona física sol·licitant d'un certificat electrònic de persona jurídica.

c) Violació o posada en perill del secret de les dades de creació de signatura del signant o del prestador de serveis de certificació o utilització indeguda d'aquestes dades per un tercer.

d) Resolució judicial o administrativa que ho ordeni.

e) Mort o extinció de la personalitat jurídica del signant; mort o extinció de la personalitat jurídica del representat; incapacitat sobrevinguda, total o parcial, del signant o del seu representat; acabament de la representació; dissolució de la persona jurídica representada o alteració de les condicions de custòdia o ús de les dades de creació de signatura que estiguin reflectides als certificats expedits a una persona jurídica.

f) Cessament en l'activitat del prestador de serveis de certificació llevat que, amb el consentiment exprés previ del signant, la gestió dels certificats electrònics expedits per aquell siguin transferits a un altre prestador de serveis de certificació.

g) Alteració de les dades aportades per obtenir el certificat o modificació de les circumstàncies verificades per expedir el certificat, com ara les relatives al càrrec o a les facultats de representació, de manera que aquest ja no sigui conforme a la realitat.

h) Qualsevol altra causa lícita prevista a la declaració de pràctiques de certificació.

2. El període de validesa dels certificats electrònics ha de ser adequat a les característiques i la tecnologia emprada per generar les dades de creació de signatura.

En el cas dels certificats reconeguts, aquest període no pot ser superior a quatre anys.

3. L'extinció de la vigència d'un certificat electrònic té efectes davant tercers, en els casos d'expiració del seu període de validesa, des que es produeixi aquesta circumstància i, en els altres casos, des que la indicació de l'extinció s'inclogui al servei de consulta sobre la vigència dels certificats del prestador de serveis de certificació.

Article 9. Suspensió de la vigència dels certificats electrònics.

1. Els prestadors de serveis de certificació han de suspendre la vigència dels certificats electrònics expedits si es dóna alguna de les causes següents:

a) Sol·licitud del signant, la persona física o jurídica representada per aquest, un tercer autoritzat o la persona física sol·licitant d'un certificat electrònic de persona jurídica.

b) Resolució judicial o administrativa que ho ordeni.

c) L'existència de dubtes fundats sobre la concurrència de les causes d'extinció de la vigència dels certificats que preveuen els paràgrafs c) i g) de l'article 8.1.

d) Qualsevol altra causa lícita prevista a la declaració de pràctiques de certificació.

2. La suspensió de la vigència d'un certificat electrònic té efectes des que s'inclogui al servei de consulta sobre la vigència dels certificats del prestador de serveis de certificació.

Article 10. Disposicions comunes a l'extinció i la suspensió de la vigència de certificats electrònics.

1. El prestador de serveis de certificació ha de fer constar immediatament, de manera clara i indubtable, l'extinció o la suspensió de la vigència dels certificats electrònics al servei de consulta sobre la vigència dels certificats quan tingui coneixement fundat de qualsevol dels fets determinants de l'extinció o la suspensió de la vigència.

2. El prestador de serveis de certificació ha d'informar el signant sobre aquesta circumstància de manera prèvia o simultània a l'extinció o la suspensió de la vigència del certificat electrònic, i ha d'especificar els motius i la data i l'hora en què el certificat quedarà sense efecte.

En els casos de suspensió, també n'ha d'indicar la durada màxima; la vigència del certificat s'extingeix si transcorre el termini esmentat i no s'ha aixecat la suspensió.

3. L'extinció o la suspensió de la vigència d'un certificat electrònic no té efectes retroactius.

4. L'extinció o la suspensió de la vigència d'un certificat electrònic s'ha de mantenir accessible al servei de consulta sobre la vigència dels certificats almenys fins a la data en què hagi finalitzat el seu període inicial de validesa.

CAPÍTOL II

Certificats reconeguts

Article 11. Concepte i contingut dels certificats reconeguts.

1. Són certificats reconeguts els certificats electrònics expedits per un prestador de serveis de certificació que compleixi els requisits que estableix aquesta Llei quant a la comprovació de la identitat i altres circumstàncies dels sol·licitants i a la fiabilitat i les garanties dels serveis de certificació que prestin.

2. Els certificats reconeguts han d'incloure, almenys, les dades següents:

a) La indicació que s'expedeixen com a tals.

b) El codi identificatiu únic del certificat.

c) La identificació del prestador de serveis de certificació que expedeix el certificat i el seu domicili.

d) La signatura electrònica avançada del prestador de serveis de certificació que expedeix el certificat.

e) La identificació del signant, en el cas de persones físiques, pel seu nom i cognoms i el seu número de document nacional d'identitat o a través d'un pseudònim que consti com a tal de manera inequívoca i, en el cas de persones jurídiques, per la seva denominació o raó social i el seu codi

d'identificació fiscal.

f) Les dades de verificació de signatura que corresponguin a les dades de creació de signatura que estiguin sota el control del signant.

g) El començament i el final del període de validesa del certificat.

h) Els límits d'ús del certificat, si s'estableixen.

i) Els límits del valor de les transaccions per a les quals es pot utilitzar el certificat, si s'estableixen.

3. Els certificats reconeguts també poden contenir qualsevol altra circumstància o atribut específic del signant en cas que sigui significatiu en funció de la finalitat pròpia del certificat i sempre que aquell ho sol·liciti.

4. Si els certificats reconeguts admeten una relació de representació han d'incloure una indicació del document públic que acrediti de forma fefaent les facultats del signant per actuar en nom de la persona o entitat a la qual representi i, en cas que sigui obligatòria la inscripció, de les dades registrals, de conformitat amb l'apartat 2 de l'article 13.

Article 12. Obligacions prèvies a l'expedició de certificats reconeguts.

Abans d'expedir un certificat reconegut, els prestadors de serveis de certificació han de complir les obligacions següents:

a) Comprovar la identitat i les circumstàncies personals dels sol·licitants de certificats d'acord amb el que disposa l'article següent.

b) Verificar que la informació que conté el certificat és exacta i que inclou tota la informació prescrita per a un certificat reconegut.

c) Assegurar-se que el signant està en possessió de les dades de creació de signatura corresponents a

les de verificació que consten al certificat.

d) Garantir la complementarietat de les dades de creació i verificació de signatura, sempre que tant les unes com les altres siguin generades pel prestador de serveis de certificació.

Article 13. Comprovació de la identitat i altres circumstàncies personals dels sol·licitants d'un certificat reconegut.

1. La identificació de la persona física que sol·liciti un certificat reconegut exigeix la personació davant els encarregats de verificar-la i s'ha d'acreditar mitjançant el document nacional d'identitat, passaport o altres mitjans admesos en dret. Es pot prescindir de la personació si la seva signatura a la sol·licitud d'expedició d'un certificat reconegut ha estat legitimada en presència notarial.

El règim de personació en la sol·licitud de certificats que s'expedeixin prèvia identificació del sol·licitant davant les administracions públiques es regeix pel que estableix la normativa administrativa.

2. En el cas de certificats reconeguts de persones jurídiques, els prestadors de serveis de certificació han de comprovar, a més, les dades relatives a la constitució i la personalitat jurídica i a

l'extensió i vigència de les facultats de representació del sol·licitant, o bé mitjançant consulta al registre públic on estiguin inscrits els documents de constitució i d'apoderament, o bé mitjançant els documents públics que serveixin per acreditar els aspectes esmentats de manera fefaent, quan no siguin d'inscripció obligatòria.

3. Si els certificats reconeguts reflecteixen una relació de representació voluntària, els prestadors de serveis de certificació han de comprovar les dades relatives a la personalitat jurídica del representat i a l'extensió i vigència de les facultats del representant, o bé mitjançant consulta al registre públic on estiguin inscrites, o bé mitjançant els documents públics que serveixin per acreditar els aspectes esmentats de manera fefaent, quan no siguin d'inscripció obligatòria. Si els certificats reconeguts admeten altres supòsits de representació, els prestadors de serveis de certificació han d'exigir l'acreditació de les circumstàncies en què es fonamentin, en la mateixa forma prevista anteriorment.

Quan el certificat reconegut contingui altres circumstàncies personals o atributs del sol·licitant, com ara la seva condició de titular d'un càrrec públic, la seva pertinença a un col·legi professional o la seva titulació, aquestes s'han de comprovar mitjançant els documents oficials que les acreditin, de conformitat amb la seva normativa específica.

4. El que disposen els apartats anteriors pot no ser exigible en els casos següents:

a) Quan la identitat o altres circumstàncies permanents dels sol·licitants dels certificats ja constin al prestador de serveis de certificació en virtut d'una relació preexistent, en la qual, per identificar l'interessat, s'hagin emprat els mitjans assenyalats en aquest article i el període de temps transcorregut des de la identificació sigui menor de cinc anys.

b) Quan per sol·licitar un certificat se n'utilitzi un altre de vigent per a l'expedició del qual s'hagi identificat el signant en la forma que prescriu aquest article i al prestador de serveis de certificació li consti que el període de temps transcorregut des de la identificació és menor de cinc anys.

5. Els prestadors de serveis de certificació poden efectuar les actuacions de comprovació que preveu

aquest article per si mateixos o per mitjà d'altres persones físiques o jurídiques, públiques o privades, i n'és responsable, en tot cas, el prestador de serveis de certificació.

Article 14. Equivalència internacional de certificats reconeguts.

Els certificats electrònics que els prestadors de serveis de certificació establerts en un Estat que no sigui membre de l'Espai Econòmic Europeu expedeixin al públic com a certificats reconeguts d'acord amb la legislació aplicable en el dit Estat es consideren equivalents als expedits pels establerts a Espanya, sempre que es compleixi alguna de les condicions següents:

a) Que el prestador de serveis de certificació compleixi els requisits que estableix la normativa comunitària sobre signatura electrònica per a l'expedició de certificats reconeguts i hagi estat certificat de conformitat amb un sistema voluntari de certificació establert en un Estat membre de l'Espai Econòmic Europeu.

b) Que el certificat estigui garantit per un prestador de serveis de certificació establert a l'Espai Econòmic Europeu que compleixi els requisits que estableix la normativa comunitària sobre signatura electrònica per a l'expedició de certificats reconeguts.

c) Que el certificat o el prestador de serveis de certificació estiguin reconeguts en virtut d'un acord bilateral o multilateral entre la Comunitat Europea i països tercers o organitzacions internacionals.

CAPÍTOL III

El document nacional d'identitat electrònic

Article 15. Document nacional d'identitat electrònic.

1. El document nacional d'identitat electrònic és el document nacional d'identitat que acredita electrònicament la identitat personal del titular i permet la signatura electrònica de documents.

2. Totes les persones físiques o jurídiques, públiques o privades, han de reconèixer l'eficàcia del document nacional d'identitat electrònic per acreditar la identitat i les altres dades personals del titular que hi constin, i per acreditar la identitat del signant i la integritat dels documents signats amb els dispositius de signatura electrònica que hi estan inclosos.

Article 16. Requisits i característiques del document nacional d'identitat electrònic.

1. Els òrgans competents del Ministeri de l'Interior per a l'expedició del document nacional d'identitat electrònic han de complir les obligacions que aquesta Llei imposa als prestadors de serveis de certificació que expedeixin certificats reconeguts, a excepció de la relativa a la constitució de la garantia a la qual es refereix l'apartat 2 de l'article 20.

2. L'Administració General de l'Estat, en la mesura que sigui possible, ha d'emprar sistemes que garanteixin la compatibilitat dels instruments de signatura electrònica inclosos al document nacional d'identitat electrònic amb els diferents dispositius i productes de signatura electrònica generalment acceptats.

TÍTOL III

Prestació de serveis de certificació

CAPÍTOL I

Obligacions

Article 17. Protecció de les dades personals.

1. El tractament de les dades personals que necessitin els prestadors de serveis de certificació per exercir la seva activitat i els òrgans administratius per exercir les funcions que atribueix aquesta Llei s'ha de subjectar al que disposen la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal, i les seves normes de desplegament.

2. Per a l'expedició de certificats electrònics al públic, els prestadors de serveis de certificació poden demanar únicament dades personals directament dels signants o previ el consentiment exprés d'aquests.

Les dades requerides han de ser exclusivament les necessàries per a l'expedició i el manteniment del certificat electrònic i la prestació d'altres serveis en relació amb la signatura electrònica, i no es poden tractar amb finalitats diferents sense el consentiment exprés del signant.

3. Els prestadors de serveis de certificació que consignin un pseudònim al certificat electrònic a sol·licitud del signant han de constatar la seva verdadera identitat i conservar la documentació que l'acrediti.

Els prestadors de serveis de certificació estan obligats a revelar la identitat dels signants quan ho sol·licitin els òrgans judicials en l'exercici de les funcions que tenen atribuïdes i en els altres supòsits que preveu l'article 11.2 de la Llei orgànica de protecció de dades de caràcter personal en què així es requereixi.

4. En qualsevol cas, els prestadors de serveis de certificació no han d'incloure als certificats electrònics que expedeixin les dades a què fa referència l'article 7 de la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal.

Article 18. Obligacions dels prestadors de serveis de certificació que expedeixin certificats electrònics.

Els prestadors de serveis de certificació que expedeixin certificats electrònics han de complir les obligacions següents:

a) No emmagatzemar ni copiar les dades de creació de signatura de la persona a la qual hagin prestat els seus serveis.

b) Proporcionar al sol·licitant abans d'expedir el certificat la informació mínima següent, que s'ha de transmetre de forma gratuïta, per escrit o per via electrònica:

1r Les obligacions del signant, la forma en la qual s'han de custodiar les dades de creació de signatura, el procediment que s'ha de seguir per comunicar la pèrdua o possible utilització indeguda de les dades i determinats dispositius de creació i de verificació de signatura electrònica que siguin compatibles amb les dades de signatura i amb el certificat expedit.

2n Els mecanismes per garantir la fiabilitat de la signatura electrònica d'un document al llarg del temps.

3r El mètode utilitzat pel prestador per comprovar la identitat del signant o altres dades que constin al certificat.

4t Les condicions precises d'utilització del certificat, els seus possibles límits d'ús i la forma en la qual el prestador garanteix la seva responsabilitat patrimonial.

5è Les certificacions que hagi obtingut, si s'escau, el prestador de serveis de certificació i els procediments aplicables per a la resolució extrajudicial dels conflictes que puguin sorgir per l'exercici de la seva activitat.

6è Les altres informacions contingudes a la declaració de pràctiques de certificació.

La informació damunt esmentada que sigui rellevant per a tercers afectats pels certificats ha d'estar disponible a instància d'aquests.

c) Mantenir un directori actualitzat de certificats en el qual s'han d'indicar els certificats expedits i si estan vigents o si la seva vigència ha estat suspesa o extingida.

La integritat del directori s'ha de protegir mitjançant la utilització dels mecanismes de seguretat adequats.

d) Garantir la disponibilitat d'un servei de consulta sobre la vigència dels certificats ràpid i segur.

Article 19. Declaració de pràctiques de certificació.

1. Tots els prestadors de serveis de certificació han de formular una declaració de pràctiques de certificació en la qual han de detallar, en el marc d'aquesta Llei i de les seves disposicions de desplegament, les obligacions que es comprometen a complir en relació amb la gestió de les dades de creació i verificació de signatura i dels certificats electrònics, les condicions aplicables a la sol·licitud, expedició, ús, suspensió i extinció de la vigència dels certificats, les mesures de seguretat tècniques i organitzatives, els perfils i els mecanismes d'informació sobre la vigència dels certificats i, si s'escau, l'existència de procediments de coordinació amb els registres públics corresponents que permetin l'intercanvi d'informació de manera immediata sobre la vigència dels

poders indicats als certificats i que hagin de figurar preceptivament inscrits en aquests registres.

2. La declaració de pràctiques de certificació de cada prestador ha d'estar disponible al públic de manera fàcilment accessible, almenys per via electrònica i de forma gratuïta.

3. La declaració de pràctiques de certificació té la consideració de document de seguretat als efectes que preveu la legislació en matèria de protecció de dades de caràcter personal i ha de contenir tots els requisits que exigeix per a aquest document la legislació esmentada.

Article 20. Obligacions dels prestadors de serveis de certificació que expedeixin certificats reconeguts.

1. A més de les obligacions establertes en aquest capítol, els prestadors de serveis de certificació que expedeixin certificats reconeguts han de complir les obligacions següents:

a) Demostrar la fiabilitat necessària per prestar serveis de certificació.

b) Garantir que es pugui determinar amb precisió la data i l'hora en què es va expedir un certificat o es va extingir o suspendre la seva vigència.

c) Ocupar personal amb la qualificació, els coneixements i l'experiència necessaris per a la prestació dels serveis de certificació oferts i els procediments de seguretat i de gestió adequats en l'àmbit de la signatura electrònica.

d) Utilitzar sistemes i productes fiables que estiguin protegits contra tota alteració i que garanteixin la seguretat tècnica i, si s'escau, criptogràfica dels processos de certificació als quals serveixen de suport.

e) Prendre mesures contra la falsificació de certificats i, en el cas que el prestador de serveis de certificació generi dades de creació de signatura, garantir-ne la confidencialitat durant el procés de generació i el lliurament per un procediment segur al signant.

f) Conservar registrada per qualsevol mitjà segur tota la informació i documentació relativa a un certificat reconegut i les declaracions de pràctiques de certificació vigents en cada moment, almenys

durant 15 anys comptats des del moment de l'expedició, de manera que es puguin verificar les signatures efectuades amb aquest.

g) Utilitzar sistemes fiables per emmagatzemar certificats reconeguts que permetin comprovar la seva autenticitat i impedir que persones no autoritzades alterin les dades, restringeixin la seva accessibilitat en els casos o a les persones que el signant hagi indicat i permetin detectar qualsevol canvi que afecti aquestes condicions de seguretat.

2. Els prestadors de serveis de certificació que expedeixin certificats reconeguts han de constituir una assegurança de responsabilitat civil per un import d'almenys 3.000.000 d'euros per respondre al risc de la responsabilitat pels danys i perjudicis que pugui ocasionar l'ús dels certificats que expedeixin.

Aquesta garantia pot ser substituïda totalment o parcialment per una garantia mitjançant aval bancari o assegurança de caució, de manera que la suma de les quantitats assegurades sigui com a mínim de 3.000.000 d'euros.

Les quanties i els mitjans d'assegurament i garantia establerts en els dos paràgrafs anteriors poden ser modificats mitjançant un reial decret.

Article 21. Cessament de l'activitat d'un prestador de serveis de certificació.

1. El prestador de serveis de certificació que cessi en la seva activitat ho ha de comunicar als signants que utilitzin els certificats electrònics que hagi expedit així com als sol·licitants de certificats expedits a favor de persones jurídiques; i pot transferir, amb el seu consentiment exprés, la gestió dels que continuïn sent vàlids en la data en què la cessació es produeixi a un altre prestador de serveis de certificació que els assumeixi o, en cas contrari, extingir la seva vigència. Aquesta comunicació s'ha de dur a terme amb una antelació mínima de dos mesos a la cessació efectiva de l'activitat i ha d'informar, si s'escau, sobre les característiques del prestador al qual es proposa la transferència de la gestió dels certificats.

2. El prestador de serveis de certificació que expedeixi certificats electrònics al públic ha de comunicar al Ministeri de Ciència i Tecnologia, amb l'antelació indicada a l'apartat anterior, la cessació de la seva activitat i la destinació que donarà als certificats, i ha d'especificar, si s'escau, si transfereix la gestió i a qui o si extingeix la seva vigència.

Igualment, ha de comunicar qualsevol altra circumstància rellevant que pugui impedir la continuació de la seva activitat. En especial, ha de comunicar, quan en tingui coneixement, l'obertura de qualsevol procés concursal que se segueixi contra ell.

3. Els prestadors de serveis de certificació han de trametre al Ministeri de Ciència i Tecnologia amb caràcter previ a la cessació definitiva de la seva activitat la informació relativa als certificats electrònics la vigència dels quals hagi estat extingida perquè aquest es faci càrrec de la seva custòdia als efectes del que preveu l'article 20.1.f). Aquest Ministeri ha de mantenir accessible al públic un servei de consulta específic on consti una indicació sobre els esmentats certificats durant un període que consideri suficient en funció de les consultes efectuades a aquest.

CAPÍTOL II

Responsabilitat

Article 22. Responsabilitat dels prestadors de serveis de certificació.

1. Els prestadors de serveis de certificació han de respondre pels danys i perjudicis que causin a qualsevol persona en l'exercici de la seva activitat quan incompleixin les obligacions que els imposa aquesta Llei.

La responsabilitat del prestador de serveis de certificació que regula aquesta Llei és exigible d'acord amb les normes generals sobre la culpa contractual o extracontractual, segons escaigui, si bé correspon al prestador de serveis de certificació demostrar que va actuar amb la diligència professional que li és exigible.

2. Si el prestador de serveis de certificació no compleix les obligacions assenyalades als paràgrafs b) al d) de l'article 12 en garantir un certificat electrònic expedit per un prestador de serveis de certificació establert en un Estat no pertanyent a l'Espai Econòmic Europeu, és responsable pels danys i perjudicis causats per l'ús d'aquest certificat.

3. De manera particular, el prestador de serveis de certificació ha de respondre dels perjudicis que es causin al signant o a tercers de bona fe per la falta o el retard en la inclusió al servei de consulta sobre la vigència dels certificats de l'extinció o suspensió de la vigència del certificat electrònic.

4. Els prestadors de serveis de certificació han d'assumir tota la responsabilitat davant tercers per l'actuació de les persones en les quals deleguin l'execució d'alguna o algunes de les funcions necessàries per prestar serveis de certificació.

5. La regulació que conté aquesta Llei sobre la responsabilitat del prestador de serveis de certificació s'entén sense perjudici del que estableix la legislació sobre clàusules abusives en contractes fets amb consumidors.

Article 23. Limitacions de responsabilitat dels prestadors de serveis de certificació.

1. El prestador de serveis de certificació no és responsable dels danys i perjudicis ocasionats al signant o tercers de bona fe, si el signant incorre en algun dels supòsits següents:

a) No haver proporcionat al prestador de serveis de certificació informació veraç, completa i exacta sobre les dades que hagin de constar al certificat electrònic o que siguin necessàries per expedir-lo o per extingir-ne o suspendre'n la vigència, quan la seva inexactitud no hagi pogut ser detectada pel prestador de serveis de certificació.

b) La falta de comunicació sense demora al prestador de serveis de certificació de qualsevol modificació de les circumstàncies reflectides al certificat electrònic.

c) Negligència en la conservació de les seves dades de creació de signatura, en l'assegurament de la seva confidencialitat i en la protecció de tot accés o revelació.

d) No sol·licitar la suspensió o revocació del certificat electrònic en cas de dubte quant al manteniment de la confidencialitat de les seves dades de creació de signatura.

e) Utilitzar les dades de creació de signatura quan hagi expirat el període de validesa del certificat electrònic o el prestador de serveis de certificació li notifiqui l'extinció o suspensió de la

seva vigència.

f) Superar els límits que figurin al certificat electrònic quant als possibles usos i a l'import individualitzat de les transaccions que es puguin realitzar amb aquest o no utilitzar-lo d'acord amb les condicions establertes i comunicades al signant pel prestador de serveis de certificació.

2. En el cas dels certificats electrònics que recullin un poder de representació del signant, tant aquest com la persona o entitat representada, quan aquesta tingui coneixement de l'existència del certificat, estan obligats a sol·licitar la revocació o suspensió de la vigència del certificat en els termes que preveu aquesta Llei.

3. Quan el signant és una persona jurídica, el sol·licitant del certificat electrònic assumeix les obligacions indicades a l'apartat 1.

4. El prestador de serveis de certificació tampoc no és responsable pels danys i perjudicis ocasionats al signant o a tercers de bona fe si el destinatari dels documents signats electrònicament actua de forma negligent.

S'entén, en particular, que el destinatari actua de forma negligent en els casos següents:

a) Quan no comprovi i tingui en compte les restriccions que figurin al certificat electrònic quant als seus possibles usos i a l'import individualitzat de les transaccions que es puguin realitzar amb aquest.

b) Quan no tingui en compte la suspensió o pèrdua de vigència del certificat electrònic publicada al servei de consulta sobre la vigència dels certificats o quan no verifiqui la signatura electrònica.

5. El prestador de serveis de certificació no és responsable dels danys i perjudicis ocasionats al signant o tercers de bona fe per la inexactitud de les dades que constin al certificat electrònic, si aquestes li han estat acreditades mitjançant un document públic. En cas que aquestes dades hagin de figurar inscrites en un registre públic, el prestador de serveis de certificació les ha de comprovar al registre esmentat en el moment immediatament anterior a l'expedició del certificat, i pot emprar, si s'escau, mitjans telemàtics.

6. L'exempció de responsabilitat davant tercers obliga el prestador de serveis de certificació a provar que va actuar en tot cas amb la diligència deguda.

TÍTOL IV

Dispositius de signatura electrònica i sistemes de certificació de prestadors de serveis de certificació i de dispositius de signatura electrònica

CAPÍTOL I

Dispositius de signatura electrònica

Article 24. Dispositius de creació de signatura electrònica.

1. Les dades de creació de signatura són les dades úniques, com ara codis o claus criptogràfiques privades, que el signant utilitza per crear la signatura electrònica.

2. Un dispositiu de creació de signatura és un programa o sistema informàtic que serveix per

aplicar les dades de creació de signatura.

3. Un dispositiu segur de creació de signatura és un dispositiu de creació de signatura que ofereix,

almenys, les garanties següents:

a) Que les dades utilitzades per generar signatura es poden produir només una vegada i assegura raonablement el seu secret.

b) Que existeix una seguretat raonable del fet que les dades utilitzades per generar signatura no poden ser derivades de les de verificació de signatura o de la mateixa signatura i del fet que la signatura està protegida contra la falsificació amb la tecnologia existent en cada moment.

c) Que les dades de creació de signatura poden ser protegides de forma fiable pel signant contra la seva utilització per tercers.

d) Que el dispositiu utilitzat no altera les dades o el document que s'hagi de signar ni impedeix que aquest es mostri al signant abans del procés de signatura.

Article 25. Dispositius de verificació de signatura electrònica.

1. Les dades de verificació de signatura són les dades, com ara codis o claus criptogràfiques públiques, que s'utilitzen per verificar la signatura electrònica.

2. Un dispositiu de verificació de signatura és un programa o sistema informàtic que serveix per aplicar les dades de verificació de signatura.

3. Els dispositius de verificació de signatura electrònica han de garantir, sempre que sigui tècnicament possible, que el procés de verificació d'una signatura electrònica satisfaci, almenys, els requisits següents:

a) Que les dades utilitzades per verificar la signatura corresponguin a les dades mostrades a la persona que verifica la signatura.

b) Que la signatura es verifiqui de forma fiable i el resultat d'aquesta verificació es presenti correctament.

c) Que la persona que verifica la signatura electrònica pugui, en cas necessari, establir de forma fiable el contingut de les dades signades i detectar si han estat modificades.

d) Que es mostrin correctament tant la identitat del signant o, si s'escau, consti clarament la utilització d'un pseudònim, com el resultat de la verificació.

e) Que es verifiquin de forma fiable l'autenticitat i la validesa del certificat electrònic corresponent.

f) Que es pugui detectar qualsevol canvi relatiu a la seva seguretat.

4. Així mateix, les dades referents a la verificació de la signatura, com ara el moment en què aquesta es produeix o una constatació de la validesa del certificat electrònic en aquell moment, poden ser emmagatzemats per la persona que verifica la signatura electrònica o per tercers de confiança.

CAPÍTOL II

Certificació de prestadors de serveis de certificació i de dispositius de creació de signatura electrònica

Article 26. Certificació de prestadors de serveis de certificació.

1. La certificació d'un prestador de serveis de certificació és el procediment voluntari pel qual una entitat qualificada pública o privada emet una declaració a favor d'un prestador de serveis de certificació, que implica un reconeixement del compliment de requisits específics en la prestació dels serveis que s'ofereixen al públic.

2. La certificació d'un prestador de serveis de certificació la pot sol·licitar aquest i la poden dur a terme, entre altres, entitats de certificació reconegudes per una entitat d'acreditació designada d'acord amb el que disposen la Llei 21/1992, de 16 de juliol, d'indústria, i les seves disposicions de desplegament.

3. En els procediments de certificació es poden fer servir normes tècniques o altres criteris de certificació adequats. En cas que es facin servir normes tècniques, s'han d'emprar preferentment les que gaudeixin d'ampli reconeixement aprovades per organismes de normalització europeus i, si no, altres normes internacionals o espanyoles.

4. La certificació d'un prestador de serveis de certificació no és necessària per reconèixer eficàcia jurídica a una signatura electrònica.

Article 27. Certificació de dispositius segurs de creació de signatura electrònica.

1. La certificació de dispositius segurs de creació de signatura electrònica és el procediment pel qual es comprova que un dispositiu compleix els requisits que estableix aquesta Llei per a la seva consideració com a dispositiu segur de creació de signatura.

2. Poden sol·licitar la certificació els fabricants o importadors de dispositius de creació de signatura i l'han de dur a terme les entitats de certificació reconegudes per una entitat d'acreditació designada d'acord amb el que disposen la Llei 21/1992, de 16 de juliol, d'indústria, i les seves disposicions de desplegament.

3. En els procediments de certificació s'han d'utilitzar les normes tècniques els números de referència de les quals hagin estat publicats en el «Diari Oficial de la Unió Europea» i, excepcionalment, les aprovades pel Ministeri de Ciència i Tecnologia que es publiquen a l'adreça d'Internet d'aquest Ministeri.

4. Els certificats de conformitat dels dispositius segurs de creació de signatura han de ser modificats

o, si s'escau, revocats quan es deixin de complir les condicions establertes per obtenir-los.

Els organismes de certificació han d'assegurar la difusió de les decisions de revocació de certificats de dispositius de creació de signatura.

Article 28. Reconeixement de la conformitat amb la normativa aplicable als productes de signatura electrònica.

1. Es presumeix que els productes de signatura electrònica esmentats al paràgraf d) de l'apartat 1 de l'article 20 i a l'apartat 3 de l'article 24 són conformes als requisits previstos en els dits articles si s'ajusten a les normes tècniques corresponents els números de referència de les quals hagin estat publicats en el «Diari Oficial de la Unió Europea».

2. Es reconeix eficàcia als certificats de conformitat sobre dispositius segurs de creació de signatura que hagin estat atorgats pels organismes designats per a això en qualsevol Estat membre de l'Espai Econòmic Europeu.

TÍTOL V

Supervisió i control

Article 29. Supervisió i control.

1. El Ministeri de Ciència i Tecnologia ha de controlar el compliment pels prestadors de serveis de certificació que expedeixin al públic certificats electrònics de les obligacions que estableixen aquesta Llei i les seves disposicions de desplegament. Així mateix, ha de supervisar el funcionament del sistema i dels organismes de certificació de dispositius segurs de creació de signatura electrònica.

2. El Ministeri de Ciència i Tecnologia ha de fer les actuacions inspectores que siguin necessàries per exercir la seva funció de control.

Els funcionaris adscrits al Ministeri de Ciència i Tecnologia que duguin a terme la inspecció a què es refereix l'apartat anterior tenen la consideració d'autoritat pública en l'acompliment de les seves comeses.

3. El Ministeri de Ciència i Tecnologia pot acordar les mesures apropiades per al compliment d'aquesta Llei i les seves disposicions de desplegament.

4. El Ministeri de Ciència i Tecnologia pot recórrer a entitats independents i tècnicament qualificades perquè l'assisteixin en les tasques de supervisió i control sobre els prestadors de serveis de certificació que li assigna aquesta Llei.

Article 30. Deure d'informació i col·laboració.

1. Els prestadors de serveis de certificació, l'entitat independent d'acreditació i els organismes de certificació tenen l'obligació de facilitar al Ministeri de Ciència i Tecnologia tota la informació i col·laboració necessàries per a l'exercici de les seves funcions.

En particular, han de permetre als seus agents o al personal inspector l'accés a les seves instal·lacions i la consulta de qualsevol documentació rellevant per a la inspecció de què es tracti, i és aplicable, si s'escau, el que disposa l'article 8.5 de la Llei 29/1998, de 13 de juliol, reguladora de la jurisdicció contenciosa administrativa. En les seves inspeccions poden anar acompanyats d'experts o perits en les matèries sobre les quals versin aquelles.

2. Els prestadors de serveis de certificació han de comunicar al Ministeri de Ciència i Tecnologia

l'inici de la seva activitat, les seves dades d'identificació, inclosa la identificació fiscal i registral, si s'escau, les dades que permetin establir comunicació amb el prestador, inclosos el nom de domini d'Internet, les dades d'atenció al públic, les característiques dels serveis que prestaran, les certificacions obtingudes per als seus serveis i les certificacions dels dispositius que utilitzin. Aquesta informació ha de ser convenientment actualitzada pels prestadors i s'ha de publicar a l'adreça d'Internet del Ministeri esmentat amb la finalitat d'atorgar-li la màxima difusió i coneixement.

3. Quan, com a conseqüència d'una actuació inspectora, es tingui coneixement de fets que puguin ser constitutius d'infraccions tipificades en altres lleis, se n'ha de donar compte als òrgans o organismes competents per a la seva supervisió i sanció.

TÍTOL VI 1.

Infraccions i sancions

Article 31. Infraccions.

1. Les infraccions dels preceptes d'aquesta Llei es classifiquen en molt greus, greus i lleus.

2. Són infraccions molt greus:

a) L'incompliment d'alguna de les obligacions que estableixen els articles 18 i 20 en l'expedició de certificats reconeguts, sempre que s'hagin causat danys greus als usuaris o la seguretat dels serveis de certificació s'hagi vist greument afectada.

El que disposa aquest apartat no és aplicable respecte a l'incompliment de l'obligació de constituir la garantia econòmica que preveu l'apartat 2 de l'article 20.

b) L'expedició de certificats reconeguts sense realitzar totes les comprovacions prèvies assenyalades a l'article 12, quan això afecti la majoria dels certificats reconeguts expedits durant els tres anys anteriors a l'inici del procediment sancionador o des de l'inici de l'activitat del prestador si aquest període és inferior.

3. Són infraccions greus:

a) L'incompliment d'alguna de les obligacions que estableixen els articles 18 i 20 en l'expedició de certificats reconeguts, excepte de l'obligació de constituir la garantia que preveu l'apartat 2 de l'article 20, quan no constitueixi infracció molt greu.

b) La falta de constitució pels prestadors que expedeixin certificats reconeguts de la garantia econòmica que preveu l'apartat 2 de l'article 20.

c) L'expedició de certificats reconeguts sense realitzar totes les comprovacions prèvies indicades a l'article 12, en els casos en què no constitueixi infracció molt greu.

d) L'incompliment pels prestadors de serveis de certificació que no expedeixin certificats reconeguts de les obligacions assenyalades a l'article 18, si s'han causat danys greus als usuaris o la seguretat dels serveis de certificació s'ha vist greument afectada.

e) L'incompliment pels prestadors de serveis de certificació de les obligacions que estableix l'article 21 respecte a la cessació d'activitat o la producció de circumstàncies que impedeixin continuar la seva activitat, quan no siguin sancionables de conformitat amb el que disposa la Llei

orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal.

f) La resistència, l'obstrucció, l'excusa o la negativa injustificada a l'actuació inspectora dels òrgans facultats per dur-la a terme d'acord amb aquesta Llei i la falta o presentació deficient de la informació sol·licitada per part del Ministeri de Ciència i Tecnologia en la seva funció d'inspecció i control.

g) L'incompliment de les resolucions dictades pel Ministeri de Ciència i Tecnologia per assegurar que el prestador de serveis de certificació s'ajusti a aquesta Llei.

4. Constitueixen infraccions lleus:

L'incompliment pels prestadors de serveis de certificació que no expedeixin certificats reconeguts de les obligacions assenyalades a l'article 18 i les restants d'aquesta Llei, quan no constitueixi infracció greu o molt greu, excepte les que conté l'apartat 2 de l'article 30.

Article 32. Sancions.

Per la comissió d'infraccions que consten a l'article anterior, s'imposen les sancions següents:

a) Per la comissió d'infraccions molt greus, s'imposa a l'infractor una multa de 150.001 a 600.000 euros.

La comissió de dues o més infraccions molt greus en el termini de tres anys pot donar lloc, en funció dels criteris de graduació de l'article següent, a la sanció de prohibició d'actuació a Espanya durant un termini màxim de dos anys.

b) Per la comissió d'infraccions greus, s'imposa a l'infractor una multa de 30.001 a 150.000 euros.

c) Per la comissió d'infraccions lleus, s'imposa a l'infractor una multa per un import de fins a 30.000 euros.

2. Les infraccions greus i molt greus poden comportar, a costa del sancionat, la publicació de la resolució sancionadora en el «Butlletí Oficial de l'Estat» i en dos diaris de difusió nacional o a la pàgina d'inici del lloc d'Internet del prestador i, si s'escau, al lloc d'Internet del Ministeri de Ciència i Tecnologia, una vegada que aquella tingui caràcter ferm.

Per imposar aquesta sanció, s'ha de considerar la repercussió social de la infracció comesa, el nombre d'usuaris afectats i la gravetat de l'il·lícit.

Article 33. Graduació de la quantia de les sancions.

La quantia de les multes que s'imposin, dins els límits indicats, es gradua tenint en compte el següent:

a) L'existència d'intencionalitat o reiteració.

b) La reincidència, per comissió d'infraccions de la mateixa naturalesa, sancionades mitjançant resolució ferma.

c) La naturalesa i la quantia dels perjudicis causats.

d) Termini de temps durant el qual s'hagi comès la infracció.

e) El benefici que hagi reportat a l'infractor la comissió de la infracció.

f) Volum de la facturació a què afecti la infracció comesa.

Article 34. Mesures provisionals.

1. En els procediments sancionadors per infraccions greus o molt greus el Ministeri de Ciència i Tecnologia pot adoptar, d'acord amb la Llei 30/1992, de 26 de novembre, de règim jurídic de les administracions públiques i del procediment administratiu comú, i les seves normes de desplegament, les mesures de caràcter provisional que s'estimin necessàries per assegurar l'eficàcia

de la resolució que definitivament es dicti, el bon final del procediment, evitar el manteniment dels efectes de la infracció i les exigències dels interessos generals.

En particular, se'n poden acordar les següents:

a) Suspensió temporal de l'activitat del prestador de serveis de certificació i, si s'escau, tancament provisional dels seus establiments.

b) Precintament, dipòsit o confiscació de registres, suports i arxius informàtics i de documents en general, així com d'aparells i equips informàtics de tot tipus.

c) Advertència al públic de l'existència de possibles conductes infractores i de la incoació de l'expedient sancionador de què es tracti, així com de les mesures adoptades per a la cessació d'aquestes conductes.

En l'adopció i el compliment de les mesures de restricció a què addudeix aquest apartat s'han de respectar, en tot cas, les garanties, les normes i els procediments previstos en l'ordenament jurídic per protegir els drets a la intimitat personal i a la protecció de les dades personals, quan puguin resultar afectats.

2. En els supòsits de danys d'excepcional gravetat en la seguretat dels sistemes emprats pel prestador de serveis de certificació que menyscabin seriosament la confiança dels usuaris en els serveis oferts, el Ministeri de Ciència i Tecnologia pot acordar la suspensió o la pèrdua de vigència dels certificats afectats, fins i tot amb caràcter definitiu.

3. En tot cas, s'ha de respectar el principi de proporcionalitat de la mesura a adoptar amb els objectius que es pretenguin assolir en cada cas.

4. En casos d'urgència i per a la protecció immediata dels interessos implicats les mesures provisionals que preveu aquest article es poden acordar abans de la iniciació de l'expedient sancionador.

Les mesures han de ser confirmades, modificades o aixecades en l'acord d'iniciació del procediment, que s'ha d'efectuar dins els 15 dies següents a la seva adopció, el qual pot ser objecte del recurs que escaigui.

En tot cas, les mesures queden sense efecte si no s'inicia el procediment sancionador en l'esmentat termini o quan l'acord d'iniciació no contingui un pronunciament exprés sobre aquelles.

Article 35. Multa coercitiva.

L'òrgan administratiu competent per resoldre el procediment sancionador pot imposar multes

coercitives per un import que no superi els 6.000 euros per cada dia que transcorri sense complir les mesures provisionals que hagin estat acordades.

Article 36. Competència i procediment sancionador.

1. La imposició de sancions per l'incompliment del que preveu aquesta Llei correspon, en el cas d'infraccions molt greus, al ministre de Ciència i Tecnologia, i en el d'infraccions greus i lleus, al secretari d'Estat de Telecomunicacions i per a la Societat de la Informació.

Això no obstant, l'incompliment de les obligacions que estableix l'article 17 el sanciona l'Agència de Protecció de Dades d'acord amb el que estableix la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal.

2. La potestat sancionadora que regula aquesta Llei s'exerceix de conformitat amb el que estableixen en aquest sentit la Llei de règim jurídic de les administracions públiques i del procediment administratiu comú i les seves normes de desplegament.

Disposició addicional primera. Fe pública i ús de signatura electrònica.

1. El que disposa aquesta Llei no substitueix ni modifica les normes que regulen les funcions que corresponen als funcionaris que tinguin legalment la facultat de donar fe en documents pel que fa a l'àmbit de les seves competències sempre que actuïn amb els requisits que exigeix la llei.

2. En l'àmbit de la documentació electrònica, correspon a les entitats prestadores de serveis de certificació acreditar l'existència dels serveis prestats en l'exercici de la seva activitat de certificació electrònica, a sol·licitud certificació en relació amb el document nacional d'identitat electrònic.

Disposició addicional segona. Exercici de la potestat sancionadora sobre l'entitat d'acreditació i els organismes de certificació de dispositius de creació de signatura electrònica.

1. En l'àmbit de la certificació de dispositius de creació de signatura, correspon al secretari d'Estat de Telecomunicacions i per a la Societat de la Informació del Ministeri de Ciència i Tecnologia imposar sancions per la comissió, pels organismes de certificació de dispositius segurs de creació de signatura electrònica o per l'entitat que els acrediti, de les infraccions greus que preveuen els paràgrafs e), f) i g) de l'apartat segon de l'article 31 de la Llei 21/1992, de 16 de juliol, d'indústria, i

de les infraccions lleus indicades al paràgraf a) de l'apartat 3 de l'article 31 de la mateixa Llei que cometin en l'exercici d'activitats relacionades amb la certificació de signatura electrònica.

2. Quan aquestes infraccions mereixin la qualificació d'infraccions molt greus, les ha de sancionar el ministre de Ciència i Tecnologia.

Disposició addicional tercera. Expedició de certificats electrònics a entitats sense personalitat jurídica per al compliment d'obligacions tributàries.

Es poden expedir certificats electrònics a les entitats sense personalitat jurídica a què es refereix

l'article 33 de la Llei general tributària únicament a l'efecte de la seva utilització en l'àmbit tributari, en els termes que estableixi el ministre d'Hisenda.

Disposició addicional quarta. Prestació de serveis per la Fàbrica Nacional de Moneda i Timbre-Reial Casa de la Moneda.

El que disposa aquesta Llei s'entén sense perjudici del que estableix l'article 81 de la Llei 66/1997, de 30 de desembre, de mesures fiscals, administratives i de l'ordre social.

Disposició addicional cinquena. Modificació de l'article 81 de la Llei 66/1997, de 30 de desembre, de mesures fiscals, administratives i de l'ordre social.

S'afegeix un apartat dotze a l'article 81 de la Llei 66/1997, de 30 de desembre, de mesures fiscals, administratives i de l'ordre social, amb la redacció següent:

«Dotze. En l'exercici de les funcions que li atribueix el present article, la Fàbrica Nacional de Moneda i Timbre-Reial Casa de la Moneda està exempta de constituir la garantia a què es refereix

l'apartat 2 de l'article 20 de la Llei 59/2003, de signatura electrònica.»

Disposició addicional sisena. Règim jurídic del document nacional d'identitat electrònic.

1. Sense perjudici de l'aplicació de la normativa vigent en matèria del document nacional d'identitat en tot el que s'adeqüi a les seves característiques particulars, el document nacional d'identitat electrònic es regeix per la seva normativa específica.

2. El Ministeri de Ciència i Tecnologia es pot adreçar al Ministeri de l'Interior perquè aquest adopti les mesures necessàries per assegurar el compliment de les obligacions que li incumbeixin com a prestador de serveis de l'usuari, o d'una autoritat judicial o administrativa.

Disposició addicional setena. Emissió de factures per via electrònica.

El que disposa aquesta Llei s'entén sense perjudici de les exigències derivades de les normes tributàries en matèria d'emissió de factures per via electrònica.

Disposició addicional vuitena. Modificacions de la Llei 34/2002, d'11 de juliol, de serveis de la societat de la informació i de comerç electrònic.

U. Addició d'un nou apartat 3 a l'article 10 de la Llei 34/2002, d'11 de juliol, de serveis de la societat de la informació i de comerç electrònic.

S'hi afegeix un apartat 3 amb el text següent:

«3. Quan s'hagi atribuït un rang de numeració telefònica a serveis de tarifació addicional en què

es permeti l'accés a serveis de la societat de la informació i es requereixi la seva utilització per part

del prestador de serveis, aquesta utilització i la descàrrega de programes informàtics que efectuïn funcions de marcació s'han de realitzar amb el consentiment previ, informat i exprés de l'usuari.

A aquest efecte, el prestador del servei ha de proporcionar almenys la informació següent:

a) Les característiques del servei que es proporciona.

b) Les funcions que efectuen els programes informàtics que es descarreguin, incloent-hi el número telefònic que s'ha de marcar.

c) El procediment per donar fi a la connexió de tarifació addicional, incloent-hi una explicació del moment concret en el qual es produirà aquest final, i

d) El procediment necessari per restablir el número de connexió previ a la connexió de tarifació addicional.

La informació anterior ha d'estar disponible de manera clarament visible i identificable.

El que disposa aquest apartat s'entén sense perjudici del que estableix la normativa de telecomunicacions, en especial, en relació amb els requisits aplicables per a l'accés per part dels usuaris als rangs de numeració telefònica, si s'escau, atribuïts als serveis de tarifació addicional.»

Dos. Els apartats 2, 3 i 4 de l'article 38 de la Llei 34/2002, d'11 de juliol, de serveis de la societat de la informació i de comerç electrònic, es redacten en els termes següents:

«2. Són infraccions molt greus:

a) L'incompliment de les ordres dictades en virtut de l'article 8 en els casos en què les hagi dictat un òrgan administratiu.

b) L'incompliment de l'obligació de suspendre la transmissió, l'allotjament de dades, l'accés a la xarxa o la prestació de qualsevol altre servei equivalent d'intermediació, quan un òrgan administratiu competent ho ordeni, en virtut del que disposa l'article 11.

c) L'incompliment significatiu de l'obligació de retenir les dades de trànsit generades per les comunicacions establertes durant la prestació d'un servei de la societat de la informació, prevista a l'article 12.

d) La utilització de les dades retingudes, en compliment de l'article 12, per a finalitats diferents de les que assenyala el dit article.

3. Són infraccions greus:

a) L'incompliment de l'obligació de retenir les dades de trànsit generades per les comunicacions establertes durant la prestació d'un servei de la societat de la informació, prevista a l'article 12, llevat que s'hagi de considerar una infracció molt greu.

b) L'incompliment significatiu del que estableixen els paràgrafs a) i f) de l'article 10.1.

c) La tramesa massiva de comunicacions comercials per correu electrònic o un altre mitjà de comunicació electrònica equivalent o la tramesa, en el termini d'un any, de més de tres comunicacions comercials pels mitjans esmentats a un mateix destinatari, quan en aquestes

trameses no es compleixin els requisits que estableix l'article 21.

d) L'incompliment significatiu de l'obligació del prestador de serveis establerta a l'apartat 1 de l'article 22, en relació amb els procediments per revocar el consentiment donat pels destinataris.

e) No posar a disposició del destinatari del servei les condicions generals a què, si s'escau, se subjecti el contracte, en la forma que preveu l'article 27.

f) L'incompliment habitual de l'obligació de confirmar la recepció d'una acceptació, quan no

s'hagi pactat la seva exclusió o el contracte s'hagi fet amb un consumidor.

g) La resistència, excusa o negativa a l'actuació inspectora dels òrgans facultats per dur-la a terme

d'acord amb aquesta Llei.

h) L'incompliment significatiu del que estableix l'apartat 3 de l'article 10.

i) L'incompliment significatiu de les obligacions d'informació o d'establiment d'un procediment de rebuig del tractament de dades, establertes a l'apartat 2 de l'article 22.

4. Són infraccions lleus:

a) La falta de comunicació al registre públic en el qual estiguin inscrits, d'acord amb el que estableix l'article 9, del nom o noms de domini o adreces d'Internet que facin servir per a la prestació de serveis de la societat de la informació.

b) No informar en la forma que prescriu l'article 10.1 sobre els aspectes assenyalats als paràgrafs

b), c), d), e) i g) del mateix article, o als paràgrafs a) i f) quan no constitueixi infracció greu.

c) L'incompliment del que preveu l'article 20 per a les comunicacions comercials, ofertes promocionals i concursos.

d) La tramesa de comunicacions comercials per correu electrònic o un altre mitjà de comunicació electrònica equivalent quan en aquestes trameses no es compleixin els requisits que estableix l'article 21 i no constitueixi infracció greu.

e) No facilitar la informació a què es refereix l'article 27.1, quan les parts no hagin pactat la seva

exclusió o el destinatari sigui un consumidor.

f) L'incompliment de l'obligació de confirmar la recepció d'una petició en els termes que estableix l'article 28, quan no s'hagi pactat la seva exclusió o el contracte s'hagi fet amb un consumidor, llevat que constitueixi infracció greu.

g) L'incompliment de les obligacions d'informació o d'establiment d'un procediment de rebuig del

tractament de dades, establertes a l'apartat 2 de l'article 22, quan no constitueixi infracció greu.

h) L'incompliment de l'obligació del prestador de serveis que estableix l'apartat 1 de l'article 22, en relació amb els procediments per revocar el consentiment prestat pels destinataris quan no constitueixi infracció greu.

i) L'incompliment del que estableix l'apartat 3 de l'article 10, quan no constitueixi infracció greu.»

Tres. Modificació de l'article 43, apartat 1, segon paràgraf de la Llei 34/2002, d'11 de juliol, de serveis de la societat de la informació i de comerç electrònic.

El segon paràgraf de l'apartat 1 de l'article 43 queda redactat de la manera següent:

«No obstant això, la imposició de sancions per incompliment de les resolucions dictades pels òrgans competents en funció de la matèria o entitat de què es tracti a què es refereixen els paràgrafs a) i b) de l'article 38.2 d'aquesta Llei correspon a l'òrgan que va dictar la resolució incomplerta.

Igualment, correspon a l'Agència de Protecció de Dades imposar sancions per la comissió de les

infraccions tipificades als articles 38.3 c), d) i i) i 38.4 d), g) i h) d'aquesta Llei.»

Quatre. Modificació de l'article 43, apartat 2 de la Llei 34/2002, d'11 de juliol, de serveis de la societat de la informació i de comerç electrònic.

L'apartat 2 de l'article 43 queda redactat de la manera següent:

«2. La potestat sancionadora que regula aquesta Llei s'ha d'exercir de conformitat amb el que estableixen en aquest sentit la Llei 30/1992, de 26 de novembre, de règim jurídic de les administracions públiques i del procediment administratiu comú, i les seves normes de desplegament. Amb tot, el termini màxim de durada del procediment simplificat és de tres mesos.»

Disposició addicional novena. Garantia d'accessibilitat per a les persones amb discapacitat i de la tercera edat.

Els serveis, els processos, els procediments i els dispositius de signatura electrònica han de ser plenament accessibles a les persones amb discapacitat i de la tercera edat, les quals no poden ser en cap cas discriminades en l'exercici dels drets i de les facultats que reconeix aquesta Llei per causes basades en raons de discapacitat o edat avançada.

Disposició addicional desena. Modificació de la Llei d'enjudiciament civil.

S'afegeix un apartat tres a l'article 326 de la Llei d'enjudiciament civil amb el tenor següent:

«Quan la part a la qual interessi l'eficàcia d'un document electrònic ho demani o s'impugni la seva

autenticitat, s'ha de procedir d'acord amb el que estableix l'article 3 de la Llei de signatura electrònica.»

Disposició transitòria primera. Validesa dels certificats electrònics expedits abans d'entrar en vigor aquesta Llei.

Els certificats electrònics que hagin estat expedits per prestadors de serveis de certificació en el marc del Reial decret llei 14/1999, de 17 de setembre, sobre signatura electrònica, mantenen la seva validesa.

Disposició transitòria segona. Prestadors de serveis de certificació establerts a Espanya abans d'entrar en vigor aquesta Llei.

Els prestadors de serveis de certificació establerts a Espanya abans d'entrar en vigor aquesta Llei han de comunicar al Ministeri de Ciència i Tecnologia la seva activitat i les característiques dels serveis que presten en el termini d'un mes des de l'entrada en vigor esmentada. Aquesta informació és objecte de publicació a l'adreça d'Internet del dit Ministeri amb la finalitat d'atorgar-li la màxima difusió i coneixement.

Disposició derogatòria única. Derogació normativa.

Queda derogat el Reial decret llei 14/1999, de 17 de setembre, sobre signatura electrònica, i totes les disposicions del mateix rang o inferior que s'oposin al que disposa aquesta Llei.

Disposició final primera. Fonament constitucional.

Aquesta Llei es dicta a l'empara de l'article 149.1.8a, 18a, 21a i 29a de la Constitució.

Disposició final segona. Desplegament reglamentari.

1. El Govern ha d'adaptar la regulació reglamentària del document nacional d'identitat a les previsions d'aquesta Llei.

2. Així mateix, s'habilita el Govern per dictar les altres disposicions reglamentàries que siguin necessàries per al desplegament i l'aplicació d'aquesta Llei.

Disposició final tercera. Entrada en vigor.

Aquesta Llei entra en vigor al cap de tres mesos de la publicació en el «Butlletí Oficial de l'Estat».

Per tant, Mano a tots els espanyols, particulars i autoritats, que compleixin aquesta Llei i que la facin complir.

Madrid, 19 de desembre de 2003.

JUAN CARLOS R.

El president del Govern,

JOSÉ MARÍA AZNAR LÓPEZ

Apèndix sobre el funcionament de l'algoritme DES

DES és un criptosistema de xifrat per blocs. El text pla original serà dividit en blocs de 64 bits, i el resultat de l'encriptació seran blocs de la mateixa mida. Cadascun dels blocs de 64 bits és dividit en dos blocs de 32 bits, el bloc de la dreta **D**, i el bloc de l'esquerra **E** (aquesta divisió es fa només en determinades operacions).

Prenem com a missatge en text pla M=0123456789ABCDEF, on **M** està escrit en hexadecimal (base 16). El missatge **M** en format binari passarà a ser un bloc de 64 bits, que és la mida que necessitem per aplicar l'algoritme DES.

M = 0000 0001 0010 0011 0100 0101 0110 0111 1000 1001 1010 1011 1100 1101 1110 1111
L = 0000 0001 0010 0011 0100 0101 0110 0111
R = 1000 1001 1010 1011 1100 1101 1110 1111

DES opera els blocs de 64 bits utilitzant claus de 56 bits. Les claus s'emmagatzemen en formats de 64 bits, però cada vuitè bit de les clau no s'utilitza, és a dir, els bits número 8, 16, 24, 32, 40, 48, 56 i 64. Als càlculs de l'exemple, s'enumeraran els bits de l'1 al 64, d'esquerra a dreta, però els bits de les posicions vuitenes seran eliminats al crear les subclaus. Per exemple, si prenem un nombre hexadecimal K= 133457799BBCDFF1, podem agrupar les xifres de 8 en 8 bits (1 = 0001, 3 = 0011, 3=0011, 4=0100,5=0101 ...) però el darrer bit de cada grup no serà utilitzat. Per tant K serà:

K = 00010011 00110100 01010111 01111001 10011011 10111100 11011111 11110001

L'algoritme DES fa els següents passos:

Pas 1: Creació de les 16 subclaus, cadascuna de les quals serà de mida 48 bits

La clau de 64 bits es permuta d'acord a la taula PC-1.

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

PC-1

A partir de la clau original K de 64 bits

K = 00010011 00110100 01010111 01111001 10011011 10111100 11011111 11110001

obtenim la permutació de 56 bits

K+ = 1111000 0110011 0010101 0101111 0101010 1011001 1001111 0001111

Ara, dividim la clau K en dos parts, dreta C_0 i esquerra D_0 de 28 bits cadascuna.

C_0 = 1111000 0110011 0010101 0101111
D_0 = 0101010 1011001 1001111 0001111

Un cop definides C_0 i D_0, crearem setze blocs C_n i D_n, on 1<=**n**<=16. Cada parell de blocs C_n i D_n es forma a partir del anterior C_{n-1} i D_{n-1} desplaçant els bits cap a l'esquerra tantes posicions com ens marca la següent taula (cada bit es mou les posicions a l'esquerra que marca la taula, excepte el primer, que cíclicament es posa a la darrera posició del bloc.).

Número d'iteració	Número de desplaçaments a l'esquerra
1	1
2	1
3	2
4	2
5	2
6	2
7	2
8	2
9	1
10	2
11	2
12	2
13	2
14	2
15	2
16	1

D'aquesta forma veiem que, per exemple C_3 i D_3 s'obtenen a partir de C_2 i D_2 respectivament aplicant dos desplaçaments a l'esquerra. C_{16} i D_{16} s'obtenen a partir de C_{15} i D_{15} respectivament aplicant un desplaçament a l'esquerra.

A partir del parell original C_0 i D_0 podem calcular la resta:

C_0 = 11110000110011001010101111
D_0 = 01010101011001100111100011111

C_1 = 1110000110011001010101011111
D_1 = 1010101011001100111100011110

C_2 = 1100001100110010101010111111
D_2 = 0101010110011001111000111101

C_3 = 0000110011001010101011111111
D_3 = 0101011001100111100011110101

C_4 = 0011001100101010101111111100
D_4 = 0101100110011110001111010101

C_5 = 1100110010101010111111110000
D_5 = 0110011001111000111101010101

C_6 = 0011001010101011111111000011
D_6 = 1001100111100011110101010101

C_7 = 1100101010101111111100001100
D_7 = 0110011110001111010101010110

C_8 = 0010101010111111110000110011
D_8 = 1001111000111101010101011001

C_9 = 0101010101111111100001100110
D_9 = 0011110001111010101010110011

C_{10} = 0101010111111110000110011001
D_{10} = 1111000111101010101011001100

C_{11} = 0101011111111000011001100101
D_{11} = 1100011110101010101100110011

C_{12} = 0101111111100001100110010101
D_{12} = 0001111010101010110011001111

C_{13} = 0111111110000110011001010101
D_{13} = 0111101010101011001100111100

C_{14} = 1111111000011001100101010101
D_{14} = 1110101010101100110011110001

C_{15} = 1111100001100110010101010111
D_{15} = 1010101010110011001111000111

C_{16} = 1111000011001100101010101111
D_{16} = 0101010101100110011110001111

Podem crear les claus K_n on 1<=**n**<=16 aplicant la taula de permutació PC-2 a cadascun dels parells C_n i D_n. Cada parell té 56 bits, però PC-2 només utilitza 48 d'aquests.

14	17	11	24	1	5

3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

PC-2

Per tant, el primer bit de K_n serà el 14é bit de c_n i D_n , el segon bit serà el 17é, fins arribar al 48é bit de K_n , que serà el 32é segons la taula PC-2.

Per a la primera clau tenim C_1 D_1 = 1110000 1100110 0101010 1011111 1010101 0110011 0011110 0011110

Després d'aplicar la permutació PC-2 obtenim

K_1 = 000110 110000 001011 101111 111111 000111 000001 110010

La resta de claus seran:

K_2 = 011110 011010 111011 011001 110110 111100 100111 100101
K_3 = 010101 011111 110010 001010 010000 101100 111110 011001
K_4 = 011100 101010 110111 010110 110110 110011 010100 011101
K_5 = 011111 001110 110000 000111 111010 110101 001110 101000
K_6 = 011000 111010 010100 111110 010100 000111 101100 101111
K_7 = 111011 001000 010010 110111 111101 100001 100010 111100
K_8 = 111101 111000 101000 111010 110000 010011 101111 111011
K_9 = 111000 001101 101111 101011 111011 011110 011110 000001
K_{10} = 101100 011111 001101 000111 101110 100100 011001 001111
K_{11} = 001000 010101 111111 010011 110111 101101 001110 000110
K_{12} = 011101 010111 000111 110101 100101 000110 011111 101001
K_{13} = 100101 111100 010111 010001 111110 101011 101001 000001
K_{14} = 010111 110100 001110 110111 111100 101110 011100 111010
K_{15} = 101111 111001 000110 001101 001111 010011 111100 001010
K_{16} = 110010 110011 110110 001011 000011 100001 011111 110101

Un cop obtingudes les subclaus, passem al missatge.

Pas 2: Xifrat dels blocs de 64 bits

Primer es realitza una permutació inicial (IP – Initial permutation) dels 64 bits del bloc del missatge **M**. Aquest canvi es fa seguint la següent taula.

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6

64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

IP

Per tant, el bit 58 del missatge **M** es converteix en el primer bit després d'aplicar la permutació inicial, el bit 50 passarà a ser el segon, i seguint la taula, fins arribar al darrer bit, que provindrà del setè del missatge M.

Aplicant aquesta permutació al missatge **M** definit anteriorment obtenim

M = 0000 0001 0010 0011 0100 0101 0110 0111 1000 1001 1010 1011 1100 1101 1110 1111
IP = 1100 1100 0000 0000 1100 1100 1111 1111 1111 0000 1010 1010 1111 0000 1010 1010

El següent pas serà dividir el bloc obtingut de la permutació en dues parts, els 32 bits de la part esquerra L_0 i els 32 de la part dreta R_0. En aquest cas:

L_0 = 1100 1100 0000 0000 1100 1100 1111 1111
R_0 = 1111 0000 1010 1010 1111 0000 1010 1010

Ara s'han de realitzar les 16 iteracions, 1<=**n**<=16, emprant la funció **f**, que opera dos blocs, un d'ells serà un bloc de dades de 32 bits, i l'altre la clau K_n de 48 bits corresponent per obtenir com a resultat un bloc de 32 bits. Denotarem l'operació **XOR (suma bit a bit mòdul 2)** amb el símbol $\oplus$. Per a les **n** rondes, des de la 1 fins a la 16, es farà servir les fórmules

$$L_n = R_{n-1}$$
$$R_n = L_{n-1} \oplus f(R_{n-1}, K_n)$$

Els resultats seran 16 blocs E_n D_n. A cadascuna de les rondes prenem els 32 bits de la dreta del resultat previ, i el fem servir com als 32 bits de l'esquerra de la ronda actual. Per als 32 bits de la dreta de la ronda actual, farem una operació XOR dels 32 bits de l'esquerra del pas anterior aplicant la funció **f**.

Per exemple, a la ronda n=1, tenim

K_1 = 000110 110000 001011 101111 111111 000111 000001 110010
L_1 = R_0 = 1111 0000 1010 1010 1111 0000 1010 1010

$$R_1 = L_0 \oplus f(R_0, K_1)$$

Cal explicar encara com funciona la funció **f**. Per al seu càlcul, primer s'ha d'expandir cada bloc R_{n-1} de 32 bits a 48. Per fer-ho, es fa servir una taula de selecció que repeteix alguns dels bits en R_{n-1}. Anomenarem l'ús d'aquesta taula com a **E**. Per tant, $E(R_{n-1})$ tindrà una entrada de 32 bits, i com a sortida un bloc de 48 bits.

Sigui E tal que, els 48 bits de la sortida, escrits en 8 blocs de 6 bits cadascun, siguin obtinguts

seleccionant els bits de l'entrada en l'ordre que ens marca aquesta taula.

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Taula de selecció E-BIT

En el nostre exemple, calcularem $E(R_0)$ a partir de R_0 de la següent forma:

R_0 = 1111 0000 1010 1010 1111 0000 1010 1010
$E(R_0)$ = 011110 100001 010101 010101 011110 100001 010101 010101

D'aquesta forma aconseguim que cadascun dels blocs de 4 bits ha sigut expandit a blocs de 6 bits a la sortida de E.

El següent pas en el càlcul **f** serà fer una operació XOR de la sortida $E(R_{n-1})$ amb la corresponent clau K_n ,

$$K_n \oplus E(R_{n-1})$$

Per tant, en el cas K_1 , $E(R_0)$:

K_1 = 000110 110000 001011 101111 111111 000111 000001 110010
$E(R_0)$ = 011110 100001 010101 010101 011110 100001 010101 010101
$K_1 \oplus E(R_0)$ = 011000 010001 011110 111010 100001 100110 010100 100111.

Feta aquesta operació XOR, continuem amb el càlcul de **f**. Donat que hem expandit R_{n-1} de 32 a 48 bits, mitjançant la taula de selecció E-BIT, i després s'ha fet una operació XOR operant aquest resultat amb la clau K_n , obtenim una sortida de 48 bits, 8 grups de 6 bits cadascun. Aquests 8 grups es faran anar com adreces en taules anomenades “Caixes-S”, o “**S-Boxes**”. Cada grup de 6 bits ens donarà una adreça en una “S-Box” diferent. En aquella adreça de la taula hi haurà representat un nombre de 4 bits. Aquest nombre de 4 bits substituirà al de 6 bits original i que ha marcat l'adreça de la S-Box. Per tant, els 8 grups de 6 bits seran reemplaçats per 8 grups de 4 bits, sorgits de les sortides de les S-Boxes, i donaran com a resultat final un nombre de 32 bits.

En el nostre exemple, escrivim el resultat previ de la següent forma:

$$K_n \oplus E(R_{n-1}) = B_1 B_2 B_3 B_4 B_5 B_6 B_7 B_8$$

Cada B_i és un dels 8 grups de 6 bits. Ara calculem

$$S_1(B_1) S_2(B_2) S_3(B_3) S_4(B_4) S_5(B_5) S_6(B_6) S_7(B_7) S_8(B_8)$$

on $S_i(B_i)$ és la sortida de cadascuna de les **i** S-Boxes.

Podem veure la taula que determina les sortides de S_1 es pot veure seguidament:

		Columnes															
		0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
	0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
Files	**1**	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
	2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
	3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S_1

Per tant, si prenem B com el bloc de 6 bits d'entrada, la sortida $S_1(B)$ serà determinada de la següent manera: Els primers i darrers bits de B representen en base 2, un nombre decimal del 0 al 3 (en binari, del 00 al 11). Denotarem aquest nombre com a **i**. Els 4 bits del mig de B, representen, en base 2, un nombre del ran decimal 0 fins al 15 (en binari, del 0000 al 1111). Denotarem aquest nombre com a **j**. Mirant a la taula, el nombre que es troba en la **fila i** i la **columna j**, serà un nombre en el rang de números decimal del 0 al 15 i és representat de forma única per un bloc de 4 bits. Aquest bloc serà la sortida de $S_1(B)$, aplicar S_1 a B. Per exemple, per un bloc d'entrada B=011011, el primer bit és “0”, i el darrer és “1”, donant 01 com la fila a triar. Els 4 bits centrals son “1101”, equivalent binari al 13. Aquest nombre serà la columna a triar. En la fila 1 i columna 13 trobem un número 5. Aquesta serà la sortida, 5 en la seva forma binària, 0101. Per tant $S_1(011011)=0101$.

Les taules que defineixen les funcions S_1 S_2 S_3 S_4 S_5 S_6 S_7 S_8

		Columnes															
		0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
	0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
Files	**1**	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
	2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
	3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S_1

		Columnes															
		0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
	0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
Files	**1**	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
	2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
	3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S_2

		Columnes															
		0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
	0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
Files	**1**	13	7	0	9	3	4	6	10	2	8	52	14	12	11	15	1
	2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
	3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

S_3

		Columnes															
		0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
	0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
Files	**1**	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
	2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
	3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

S_4

		Columnes															
		0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
	0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
Files	**1**	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
	2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
	3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

S_5

		Columnes															
		0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
	0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
Files	**1**	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
	2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
	3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

S_6

		Columnes															
		0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
	0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
Files	**1**	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
	2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
	3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

S_7

		Columnes														
		0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
	0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
Files	**1**	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
	2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
	3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

S_8

En l'exemple, a la primera ronda obtindrem el següent resultat a la sortida de les S-Boxes:

$K_1 \oplus L(R_0)$ = 011000 010001 011110 111010 100001 100110 010100 100111.

$S_1(B_1)S_2(B_2)S_3(B_3)S_4(B_4)S_5(B_5)S_6(B_6)S_7(B_7)S_8(B_8)$ = 0101 1100 1000 0010 1011 0101 1001 0111

La part final del càlcul **f** és una permutació P de la sortida de les S-Boxes:

$f = P(S_1(B_1)S_2(B_2)S_3(B_3)S_4(B_4)S_5(B_5)S_6(B_6)S_7(B_7)S_8(B_8))$

Aquesta permutació P està definida per la següent taula P, que, a partir d'una entrada de 32 bits, dóna com a sortida un altre bloc de 32 bits obtingut de la permutació dels bits del bloc d'entrada.

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

P

Seguint amb l'exemple, de la sortida de les S-Boxes

$S_1(B_1)S_2(B_2)S_3(B_3)S_4(B_4)S_5(B_5)S_6(B_6)S_7(B_7)S_8(B_8)$ = 0101 1100 1000 0010 1011 0101 1001 0111

obtindrem

$f = P(S_1(B_1)S_2(B_2)S_3(B_3)S_4(B_4)S_5(B_5)S_6(B_6)S_7(B_7)S_8(B_8))$ = 0010 0011 0100 1010 1010 1001 1011 1011

$R_1 = L_0 \oplus f(R_0, K_1)$ = 1100 1100 0000 0000 1100 1100 1111 1111
+ 0010 0011 0100 1010 1010 1001 1011 1011
= 1110 1111 0100 1010 0110 0101 0100 0100

En la següent ronda tindrem que és el bloc que acabem de calcular. Ara calcularem $R_2 = L_1 \oplus f(R_1, K_2)$, i seguirem els mateixos passos fins a la ronda 16. En acabar aquesta setzena ronda, tenim els blocs L_{16} i R_{16} . Ara s'intercanvia l'ordre dels dos blocs, formant un bloc de 64 bits $R_{16}L16$ i s'aplica la permutació final. Aquesta permutació final és la inversa de la

permutació inicial del criptosistema, IP^{-1} i està definit per la següent taula:

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

IP^{-1}

La sortida tindrà com a primer bit, el bit número 40 de la entrada a la permutació, el segon bit serà el vuitè de l'entrada, i així successivament seguint la taula.

En l'exemple, després de processar els 16 blocs amb el mètode definit anteriorment, obtenim en la ronda 16

L_{16} = 0100 0011 0100 0010 0011 0010 0011 0100

R_{16} = 0000 1010 0100 1100 1101 1001 1001 0101

Intercanviem l'ordre dels dos blocs i apliquem la permutació final:

$R_{16}L_{16}$ = 00001010 01001100 11011001 10010101 01000011 01000010 00110010 00110100

IP^{-1} = 10000101 11101000 00010011 01010100 00001111 00001010 10110100 00000101

que en format hexadecimal serà 85E813540F0AB405.

Per tant, per al missatge en clar **M** = 0123456789ABCDEF, el missatge encriptat en DES serà **C** = 85E813540F0AB405.

El mètode de desxifrat consisteix en aplicar la inversa de l'encriptació, seguint els mateixos passos descrits però en ordre invers, i invertint l'ordre en que les subclaus s'apliquen.